Administrator's Guide

Netscape Messaging Server 4.0

Version 1.0

Netscape Communications Corporation ("Netscape") and its licensors retain all ownership rights to the software programs offered by Netscape (referred to herein as "Software") and related documentation. Use of the Software and related documentation is governed by the license agreement accompanying the Software and applicable copyright law.

Your right to copy this documentation is limited by copyright law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Netscape may revise this documentation from time to time without notice.

THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL NETSCAPE BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING FROM ANY ERROR IN THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY LOSS OR INTERRUPTION OF BUSINESS, PROFITS, USE, OR DATA.

The Software and documentation are copyright ©1999 Netscape Communications Corporation. All rights reserved.

The Software contains encryption software from RSA Data Security, Inc. Copyright © 1994, 1995 RSA Data Security, Inc. All rights reserved. Portions of the Software copyright © 1995 PEER Networks, Inc. All rights reserved. Portions of the Software copyright 1991-1997 Compuware Corporation. Powered by Java technology from Sun Microsystems, Inc. Copyright © 1992-1997 Sun Microsystems, Inc. All rights reserved. Java is a trademark or registered trademark of Sun Microsystems, Inc in the United States and other countries.

Netscape, Netscape Navigator, Netscape Certificate Server, Netscape DevEdge, Netscape FastTrack Server, Netscape ONE, SuiteSpot, and the Netscape N and Ship's Wheel logos are registered trademarks of Netscape Communications Corporation in the United States and other countries. Other Netscape logos, product names, and service names are also trademarks of Netscape Communications Corporation, which may be registered in other countries. Other product and brand names are trademarks of their respective owners.

The downloading, exporting, or reexporting of Netscape software or any underlying information or technology must be in full compliance with all United States and other applicable laws and regulations. Any provision of Netscape software or documentation to the U.S. Government is with restricted rights as described in the license agreement accompanying Netscape software.

Recycled and Recyclable

Version 1.0

Part Number

©1999 Netscape Communications Corporation. All Rights Reserved
Printed in the United States of America. 01 00 99 5 4 3 2 1

Netscape Communications Corporation
501 East Middlefield Road
Mountain View, CA 94043

Contents

Chapter

1

Getting Started with Netscape Messaging Server

Welcome to Netscape Messaging Server 4.0. Messaging Server provides a powerful and flexible cross-platform solution to the email needs of enterprises and messaging hosts of all sizes. It uses an open, Internet-standard approach to messaging while providing lightning-fast processing of messages that is scalable to many thousands of simultaneous users.

This chapter describes how to get started administering Messaging Server 4.0, from installation through basic configuration of general messaging capabilities. It concludes with references to other chapters that contain configuration instructions and procedures for managing your server and your community of mail users.

This chapter has the following sections:

- Messaging Server Features
- Deployment and Installation
- Using Netscape Console
- Using the Command Line
- Configuring General Messaging Capabilities
- Where to Go from Here
- Interface Reference: General Messaging Services

Messaging Server Features

Netscape Messaging Server 4.0 is the fourth generation of a powerful, standards-based Internet mail server. Messaging Server is designed for high-capacity, reliable handling of the messaging needs of both enterprises and service providers of all sizes, from small to extremely large.

The server consists of several modular, independently configurable components with many powerful features, including these:

Highly scalability with standard protocols:

- Fast and reliable, multithreaded message transfer agent (MTA) that uses Internet-standard Simple Mail Transfer Protocol (SMTP) to handle both internal and Internet mail messages
- Extremely efficient, high-capacity, and fast multithreaded Internet Mail Access Protocol (IMAP4) service for mailbox delivery, supporting thousands of simultaneous users
- Full-featured, fast, multithreaded Post Office Protocol (POP3) service for mailbox delivery, providing complete support for the most widely used Internet mailbox protocol
- Centralized database for server configuration, based on the Lightweight Directory Access Protocol (LDAP)
- Centralized LDAP database for mail-user account storage, user authentication, and mail-routing control
- High scalability of services to support greatly increased usage over time

Flexible configuration and monitoring:

- Flexible message store with fast indexed access, configurable partitions, quotas, and aging rules
- Highly configurable logging features with automated rollover
- Monitoring capabilities through Simple Network Management Protocol (SNMP)
- Multiplexor service for providing mail users a single point of connection to many POP and IMAP mailbox servers
- Plug-in architecture for developing extensions to server capabilities
- Mailstone stress-testing utility for capacity planning and testing

Powerful security and access control:

- Support for password login (to POP, IMAP, or SMTP) and certificate-based login

- Delegated administration through access-control instructions (ACIs)
- Client access filters (to POP, IMAP, or SMTP)
- Filtering of unsolicited bulk email (UBE)

Convenient Management Interface:

- Graphical Netscape Console interface for managing multiple servers from a single location
- End-user self-management of account information through HTML forms

Procedures for configuring these and other features are described in this book. Depending on the current status of your messaging deployment, you may want to start with one of the following sections in this chapter:

- If you have already installed Netscape Messaging Server and are ready to start configuring it, see Configuring General Messaging Capabilities.
- If you want information about using the Netscape Console graphical interface or the command line to configure and run Netscape Messaging Server, see Using Netscape Console or Using the Command Line.
- If you are interested in an overview of the process of deploying and installing Netscape Messaging Server, see the next section, Deployment and Installation.

Deployment and Installation

Before you can administer a server, its place in a deployment scheme must be determined and it must be installed. This section gives an overview of the issues involved in designing and installing a messaging solution with Netscape Messaging Server. It outlines some important deployment concepts and installation configurations to be considered, and then summarizes the installation process for a single server.

For complete documentation on Messaging Server installation, see *Installing Messaging Server 4.0*. For more in-depth information on the deployment and installation-configuration topics presented here, see *Managing Servers with Netscape Console,* and Chapter 9, Message Routing, in this book.

Deployment Considerations

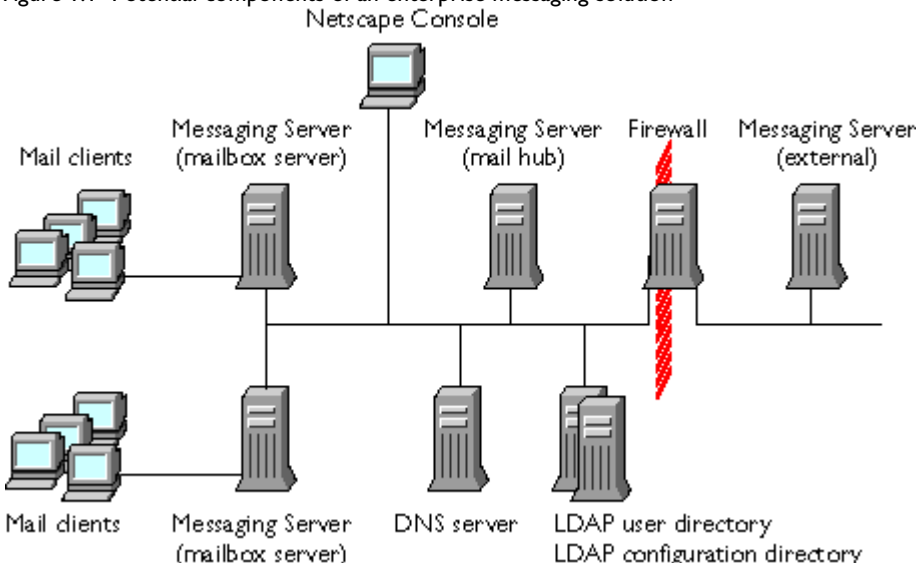
A successful messaging installation requires careful planning and execution. This section discusses some of the most basic topics to be considered in implementing a messaging solution with Messaging Server, including

- calculation of network topologies and server sizes
- resolution of host names for routing messages among servers
- resolution of user names for routing messages to mailboxes
- deployment of additional servers for specialization and redundancy
- integration of messaging with firewall security
- creation and migration of mail accounts

This is not an exhaustive list of topics, and the discussion here won't by itself allow you to design and deploy a messaging solution; it provides only a context for subsequent server-specific discussions. For more in-depth information, consult the references listed with each topic.

Each installed Messaging Server is one component of the messaging solution implemented for your enterprise. Figure 1.1 is a simplified diagram of the principal components that might be found in an enterprise messaging solution. (Service providers may have additional components, as discussed in Enterprise vs. ISP Topologies.) How your Messaging Server needs to interact with clients, with other Messaging Servers, and with the other components shown in Figure 1.1 will affect how you install, configure, and maintain the server.

Figure 1.1 Potential components of an enterprise messaging solution



Sizing and Topology

Messaging installations that use Netscape Messaging Server are highly scalable. One or more servers can be organized into a messaging infrastructure that supports anywhere from a few users up to potentially millions of users.

Designing the network topology for a messaging solution, and calculating the numbers and sizes of host machines and server instances required (both today and in the foreseeable future), is a basic deployment task. It is also, typically, an iterative process.

One way to start is by relating your total user base to basic server capacity information:

1. Start by assuming your total anticipated number of users.

2. Estimate your peak load: how many of your users need simultaneous access their POP or IMAP mailboxes? Compare that to benchmark results of the maximum number of simultaneous connections possible with Messaging Server 4.0 on a given hardware configuration. Given those figures, estimate how many servers you need to handle your users.

3. Estimate your message traffic: how many total messages need to be sent through your messaging system per day? Compare that to benchmark results of the maximum message-transfer rate possible with Messaging Server 4.0 on a given hardware configuration. Given those figures, estimate how many servers you need to handle the message flow.

Note that benchmark studies and field deployments have shown that a single Messaging Server, installed on a moderately powerful, single-processor, dedicated server host machine with sufficient memory and storage, can, under optimum conditions, support several thousand users and deliver tens to hundreds of thousands of messages per day. Furthermore, these figures scale to much higher numbers as you add more processors to the host machine.

Initial estimates you make in this way are just the start of a sizing effort. Messaging Server and the other components it relies on function in a complex network of interactions, and requirements for specialization and redundancy can add further complexity. Multiple stages of recalculation, including actual field testing, are required as additional components and refinements are brought into the design.

Your Netscape representative can also help you address sizing questions, both for a new installation and for scaling existing installations to meet added demand. Consultants from Netscape's Worldwide Professional Services are also available to help design and implement installations of any size or complexity.

Role of DNS

The Domain Name Service (DNS) is an integral part of Internet communication; it converts names to machine addresses. DNS is a requirement for routing mail in a Netscape messaging installation. Unix and Windows NT operating-system vendors make DNS available with their operating systems. For complete information on setting up and using DNS, see *DNS and BIND, 2nd ed.,* by Paul Albitz and Cricket Liu (O'Reilly).

Your enterprise must have at least one DNS server (the primary server) that has authoritative information for the names in your domain. You can have other DNS servers as well, on several host machines in several locations. Your DNS servers may be on machines dedicated to DNS or on machines with other responsibilities as well. Firewall machines are commonly used also as DNS servers.

Fundamentally, DNS translates host names and domain names to IP addresses, and vice versa. DNS uses Address (A) records for this purpose. Therefore, you need to make sure that your DNS server has A records for all Messaging Server hosts in your enterprise.

Secondarily, DNS can also translate domain names and host names to other host names. DNS uses Mail Exchange (MX) records for this purpose. This feature allows you to create private domains and to use domain-based email addresses (such as `sandee@airius.com`) instead of host-specific email addresses (such as `sandee@mail1.airius.com`).

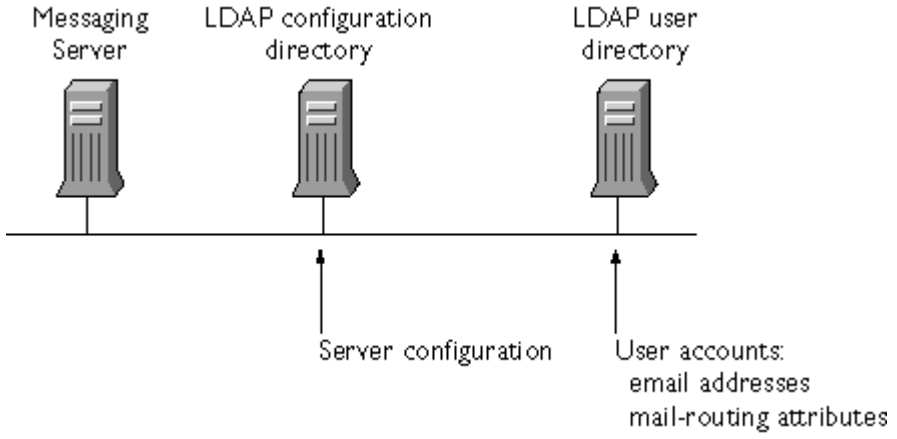
The way you set up DNS affects which of your servers first handle incoming messages, which ones pass outgoing messages to external recipients, and how messages within the enterprise get to the right mailbox server. For details on setting up A records and MX records, see Chapter 9, Message Routing.

SMTP routing table. Each Messaging Server instance keeps a local SMTP routing table that, in addition to DNS, can determine the proper destination server for a message based on the recipient's address or domain. Entries in the routing table are optional, but they provide a method for directly transferring messages from one server to another. Routing-table entries are commonly used, for example, to directly transfer all outside messages to a firewall server. For more information, see Chapter 9, Message Routing.

The Role of the LDAP Directory

Messaging Server 4.0 requires the use of an LDAP directory, such as Netscape Directory Server, for storing both server-configuration settings and mail-account information (Figure 1.2). A Directory Server must already have installed somewhere on your network before you can install Messaging Server.

Figure 1.2 User directory and configuration directory



The LDAP user directory in which your Messaging Server stores account information is typically on a separate host machine. A single Directory Server can manage the user directory for a very large organization, although for performance reasons all or parts of the directory are often replicated to one or more other machines. Setting up a directory is covered in detail in *Directory Server Deployment Guide* and *Directory Server Administrator's Guide*.

The entry for each user's account in the user directory includes mail-addressing and mail-routing attributes for that account. Whenever Messaging Server receives a message, it checks the user directory to make sure that the recipient's mail address (such as `sandee@airius.com`) exists in the directory; if it does, Messaging Server routes the mail to the recipient's host server, also indicated in the directory entry. Routing the message may involve rewriting the mail address.

The process that Messaging Server uses to match a user in the directory with an email address can be complex. You can specify at least the following attributes for each user's directory entry: primary mail address, alternate mail addresses, mail host, and mail-routing address. For detailed information on how Messaging Server uses these mail-related attributes, see Chapter 9, Message Routing.

Separation of Services

For increased performance and security, large enterprises may want to separate their messaging services by placing them on different host machines. As noted in Figure 1.1, for example, mailbox services might be separated from

centralized message-transfer services at a mail hub. Furthermore, different mailbox servers might be specialized for only POP or only IMAP. Other enterprises might in addition separate outgoing messages from incoming messages, channeling them through different SMTP mail hubs.

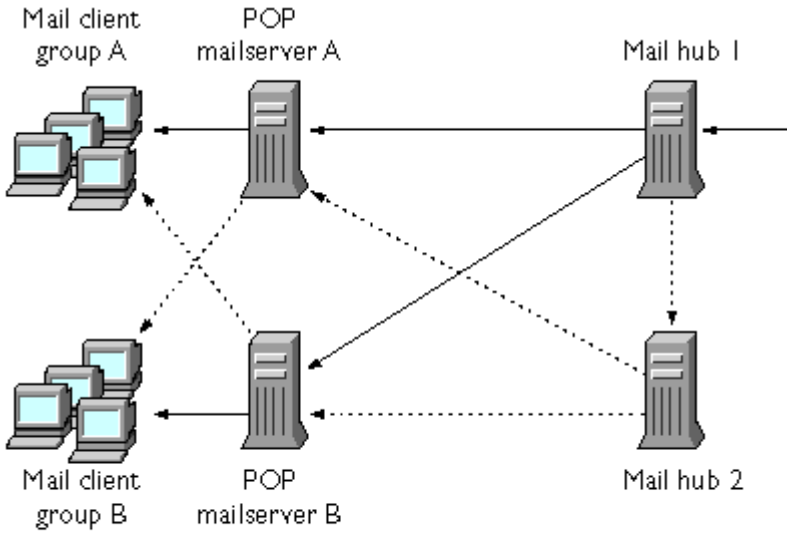
Such specializations increase the total number of servers and hosts in the enterprise and can greatly increase the complexity of routing configurations. As a result, directory services, DNS records, and SMTP routing tables need careful setup.

Redundancy Requirements

Server software is not perfect, nor are the host machines and network hardware it relies on. Almost any enterprise needs to plan for backup and for failover in case any of its important servers go down.

Therefore, in designing a messaging installation, be sure to consider the consequences of a failure of each individual Messaging Server and its host machine. Usually this means providing extra, redundant machines that can automatically take over a given server's tasks if it should fail. In installations in which messaging is distributed among specialized machines, servers already used to implement distributed functionality and replication can also function as failover servers (see Figure 1.3.)

Figure 1.3 Redundancy in a portion of a messaging installation



Designing your messaging topology for redundancy and setting up automatic failover capability can add greater complexity to an already complex configuration in a large installation.

Firewalls and Messaging

Most enterprises connected to the Internet maintain some form of firewall, a hardware or software barrier intended to prevent unauthorized external users from accessing the enterprise's servers and host machines. You can increase security by locating Messaging Servers behind the firewall, and channeling all mail access to the enterprise through one or more mail hubs, as shown in Figure 1.1. Channeling all outgoing mail through another hub provides additional control and security, allowing you to rewrite addresses or otherwise control information that leaves your enterprise.

For enterprises that receive a large volume of external mail, it might be optimal to place one Messaging Server, containing only publicly accessible accounts, outside the firewall. That server in turn would have limited access to internal servers, across the firewall, for forwarding messages to internal accounts.

Using a setup with mail hubs communicating across a firewall requires careful setup of firewall routing configurations, DNS services, and possibly SMTP routing tables to handle the complex routing possibilities. If you place a mail server outside the firewall, you might need to use a separate, external, directory server as well.

Creation and Migration of Mail Accounts

Installing Messaging Server does not by itself create any user or group accounts or migrate existing proprietary mail accounts to the user directory. Messaging Server provides the Netscape Console graphical interface for entering user and group information for individual accounts; it provides command-line utilities for batch migration of large numbers of users to Netscape messaging from existing mail systems.

For instructions on how to enter and modify mail-related attributes in the user directory, see Chapter 4, Managing Mail Users and Mailing Lists. For instructions on migrating `sendmail` user accounts to the LDAP user directory, see Appendix C, sendmail Migration and Compatibility.

Enterprise vs. ISP Topologies

Enterprises with messaging intranets for employees are similar to Internet service providers (ISPs) with messaging hosting for subscribers, in that can both be required to support many thousands of accounts and a high volume of daily traffic. Typical network topologies and server configurations may differ, however.

For example, an enterprise might have many internal, directly connected mail users, with client machines and mail hosts located mostly inside the company firewall. Domain names may relate directly to host IP addresses. Client connections to mail servers may be frequent and heavy during the day, but drop off sharply after hours. Clients may stay connected for long periods.

An ISP, on the other hand, may have many servers but very few onsite client machines. Its customers typically retrieve their mail through dial-up connections. The ISP may offer custom domain services and thus may have multiple server instances per physical host machine. At the same time, ISPs may want to isolate users from specific mail hosts and thus are more likely to use a solution like Messaging Multiplexor. ISPs may have a larger proportion of mailbox servers to hubs than do most enterprises. Redundancy for 100% reliability may be even more important to an ISP than to many enterprises. Client connections to the mail servers may be less frequent and shorter in duration, but they also may be spread out over more hours during the day, especially during the evening. ISPs, even more than enterprises, may be concerned with denying access to unauthorized users and filtering out unsolicited bulk email (UBE) to keep it from filling their customers' mailboxes.

Differences like these all have effects on the implementation of mail-routing strategies, access-filtering techniques, server-performance tuning, and server-installation configuration. For more information on access filtering and UBE filtering, see Chapter 2, Configuring IMAP and POP Services, and Chapter 8, Filtering Unsolicited Bulk Email, in this book.

Installation Configurations

To deploy a messaging solution that meets your needs and addresses the issues raised in the previous section, you may need to install Netscape Messaging Server on different host machines in different installation configurations. Depending on the size and purpose of your enterprise and the nature of your network and system hardware, your messaging deployment can consist of one

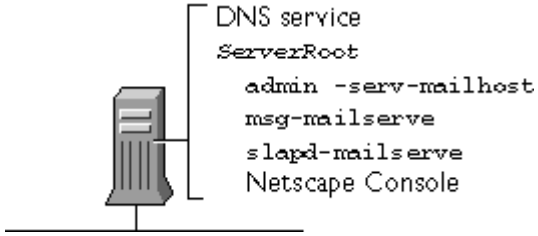
or many instances of Messaging Server, on one or many host machines, with identical or different messaging capabilities. Required supporting software--such as Netscape Console, Administration Server, Directory Server, and the DNS service--may also be concentrated or distributed across your network.

This section summarizes the common Messaging Server installation configurations. For more detailed information on installation configuration and on the interaction between Netscape Messaging Server and other services, see *Managing Servers with Netscape Console*. For additional information on LDAP directories and the Netscape Directory Server, see the Directory Server documentation.

All Services on One Host

A one-host configuration (shown in Figure 1.4) can be practical for smaller installations. It economizes on server hardware at the expense of performance and capacity. (It also provides no backup, should the one server fail.)Nevertheless, it is possible to use a single host machine to house everything. Note that, in this configuration, the single *server root* (the directory into which all Netscape servers are installed) contains the three required Netscape servers--Messaging Server, Directory Server, and Administration Server--as a single *server group* (the set of servers managed by a single Administration Server). The single Directory Server in this case manages both the *user directory* (which contains mail-account information) and the *configuration directory* (which contains server-configuration information). The DNS service and Netscape Console are also on the same host machine.

Figure 1.4 All messaging-related services on a single host

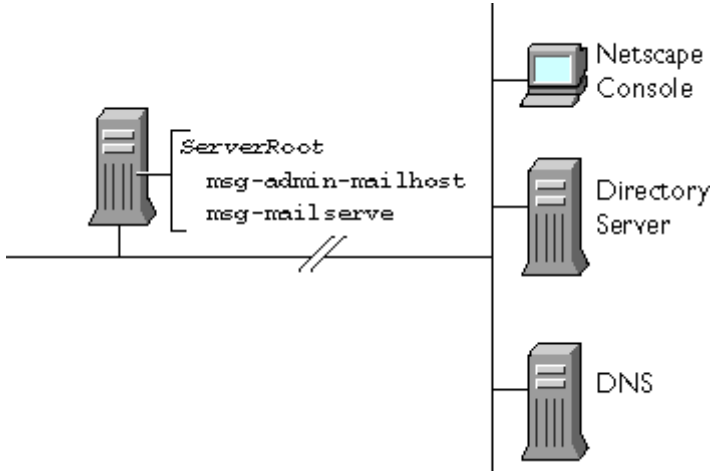


In this configuration the one host machine must have sufficient performance capacity to handle all services without undue strain. It must also have sufficient storage capacity to hold all messages and all directory information for the enterprise.

One Messaging Server per Dedicated Host

A common deployment configuration is to have a dedicated host machine for each Messaging Server instance. As Figure 1.5 shows, the LDAP directory (or directories, if user and configuration directories are separated), the DNS service, and possibly Netscape Console are on separate hosts from the installed Messaging Server. There may be one or several messaging host machines, but each contains a single server root in which a single Messaging Server and its Administration Server make up the server group.

Figure 1.5 Single Messaging Server on a single host

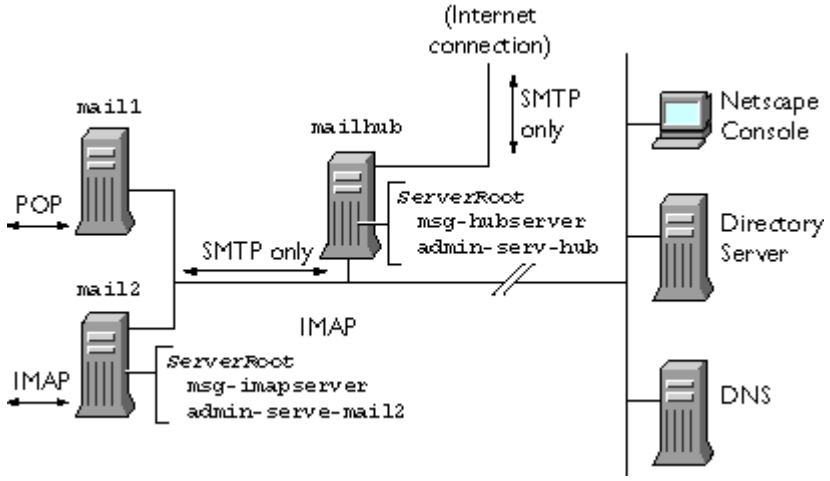


This configuration allows for optimizing each server host machine for strictly messaging tasks. Different divisions or offices of the enterprise may each have their own Messaging Server in a configuration like this one, perhaps with all servers accessing a single user directory on a dedicated host machine.

Specialized Messaging Services on Each Host

Another common deployment configuration, especially in larger installations, is to implement only certain messaging services on each host machine. As shown in Figure 1.6, for example, a centralized mail hub server, using only SMTP, connects to individual mailbox servers that use only POP or only IMAP to send mail to their users.

Figure 1.6 Mail hub and mailbox servers on separate hosts

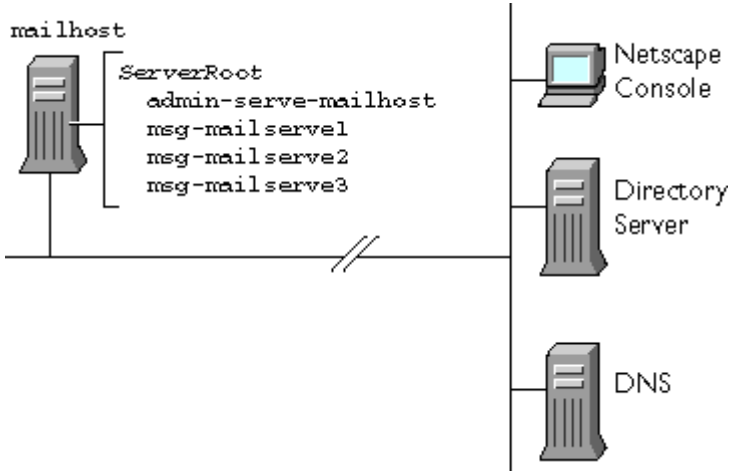


This configuration can increase security (because outsiders can connect only at one point, the mail hub), and it allows for optimizing each server machine for the specific service (SMTP, POP, IMAP) that it supports.

Multiple Server Instances per Host

If appropriate for your needs, you can install multiple server instances on a single host machine. As the example in Figure 1.7 shows, a single server root contains a server group consisting of one Administration Server and multiple instances of Messaging Server. All Messaging Server instances run from a single installed set of executable programs and libraries.

Figure 1.7 Multiple instances of Messaging Server on a single host

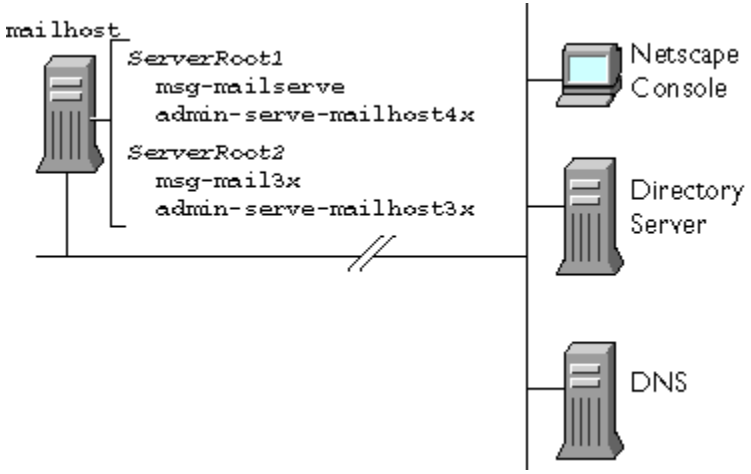


This configuration allows multiple custom domain names to be created for a single machine that has a single IP address. A host machine in this configuration must have sufficient capacity to execute and store messages from all the server instances.

Multiple Server Roots per Host

If a single host machine includes Netscape servers that have different version numbers, it may be necessary to create separate server groups, and thus separate server root directories, on the machine. Figure 1.8 shows an example in which some employees in an enterprise are using Netscape Messaging Server 3.0, while others have upgraded to Netscape Messaging Server 4.0. Both servers are running on the same host machine.

Figure 1.8 Two versions of Messaging Server on a single host



This configuration may be necessary because different versions of Messaging Server may require different directory structures or different versions of the Administration Server. The Netscape Server Setup program facilitates this configuration, letting you create a separate server root when you install new servers and leaving an existing server root undisturbed.

This configuration is commonly used for pilot deployment of new server versions, for creating a temporary setup until all users migrate to the newer version, or even for failover protection, with different server instances stored on different physical storage devices.

The Installation Process

All Netscape servers, and also the Netscape Console application that you use to manage them, are installed by running the Netscape Server Setup program. The program is provided with every Netscape server product.

This section only summarizes the installation process. For detailed instructions on installing Netscape Messaging Server, see the document *Installing Messaging Server 4.0* (file `Install.htm`) in your installation package. For additional general information on the Netscape Server Setup Program, see *Managing Servers with Netscape Console*.

Before you install Messaging Server, your Netscape Directory Server (version 3.1 or later) must be installed and your DNS service set up. Then you can install Messaging Server onto its host machine.

In summary, take these steps:

1. Obtain the Messaging Server installation package and unpack the files.

   Whether you have obtained the package from a CD-ROM or through a network download, copy the package into a temporary directory and unpack the files into that directory.

2. Configure your LDAP Directory Server appropriately for messaging, using the tools provided.

   The configuration tools add Messaging Server schema extensions to the configuration directory and prepare it for holding server-configuration information for this server instance.

3. Run the Netscape Server Setup Program (`setup`).

   Read the Welcome message and the Licensing Agreement, select the products to be installed (servers, components, or Netscape Console), choose a level of installation (Express, Typical, or Custom), and answer the prompts.

   If this is the first installation of Netscape servers on this host machine, the setup program also installs an instance of Netscape Administration Server. See *Managing Servers with Netscape Console* for information on how the Administration Server works and how to install and configure it.

4. At the last prompt, confirm the correctness of the information you have entered.

   At this point, the installer extracts the appropriate files, configures the Administration Server (if it is being installed) and the Messaging Server, and starts the servers.

Installation is complete. You can now use Netscape Console (see Using Netscape Console) to continue configuring the server (see Configuring General Messaging Capabilities and Where to Go from Here).

Silent Install. You can use the Netscape Server Setup program, along with a special configuration file, to install Messaging Server in a non-interactive mode that does not require your continued presence at the machine on which the installation occurs. If you have many similar server configurations to set up, you

can place the configuration file plus the server installation package on each machine. You execute the setup program on each machine; it then extracts all information it needs from the configuration file as it performs the installation.

Whenever you perform a manual installation, the setup program creates a log file that you can use as the configuration file for subsequent silent installs. See *Installing Messaging Server 4.0* for more information.

Console-only installation. You can use the Netscape Server Setup program to install the Netscape Console alone, so that you can use it from a client machine for remote administration. The Setup program can also install Messaging Server patches and updates. See *Installing Messaging Server 4.0* for details.

Post-Installation Directory and File Organization

Once you have installed Messaging Server 4.0, its directories and files are arranged in the organization depicted in Table 1.1. The table is not exhaustive; it shows only those directories and files of most interest for typical server administration tasks.

> **Note:** Where pathnames for Windows NT and Unix installations are identical except for separator symbols, only the Unix version is shown. Where they differ materially, both are shown. Metavariables (replaceable text strings) in pathnames are shown in italics.

Table 1.1 Important Messaging Server directories and files

Directory or file	Default or required location	Explanation
server root directory (*serverRoot*)	**Unix:** `usr/netscape/server4/` (default location)	The directory into which all servers of a given server group (that is, all servers managed by a given Administration Server) are installed. This may include other Netscape servers in addition to Messaging Server.
installation directory (*installDirectory*)	*serverRoot*`/bin/msg/` (required location)	The directory containing the binary (executable) files of the installed Messaging Server
instance directory (*instanceDirectory*)	*serverRoot*`/msg-`*instanceName*`/` (required location) where *instanceName* is the name of this instance of Messaging Server, as specified at installation. (Default = host name of server machine)	The directory containing the configuration files that define a given instance of Messaging Server. Multiple instances of Messaging Server, all using the same binary files, may exist on a given host machine.
message queue directory	*instanceDirectory*`/queue/` (default location)	The directory that holds the message queues, the temporary holding areas for received messages. See Managing the Message Queue for more details.
message store directory	*instanceDirectory*`/store/` (default location)	The directory that holds the user mailboxes. See Managing the Message Store for more details.

Table 1.1 Important Messaging Server directories and files (Continued)

Directory or file	Default or required location	Explanation
user mailbox	*instanceDirectory*/store/partition/primary/=user/userID/*subMailbox*/ where *userID* is the mail ID of the user, and *subMailbox* is the POP or IMAP folder (such as INBOX) (required location)	The location within the message store of a given mailbox directory. See Managing the Message Store for more details.
administrative command-line utilities	*installDirectory*/admin/bin/ (required location)	The directory containing command-line utilities that handle most aspects of server configuration and management. See Command-line Utilities for more details.
storage-related command-line utilities	*installDirectory*/store/bin/ (required location)	The directory containing command-line utilities that handle mail delivery and storage-database management. See Command-line Utilities for more details.
start-stop utility	**Unix:** /etc/NscpMsg (required location) **Windows NT:** Control Panel-> Services->Start or Stop (required location)	A Unix-only utility that starts and stops Messaging services. See Command-line Utilities for more details.
local configuration file	*instanceDirectory*/config/configdb (required location for Unix, default location for NT)	A file containing locally stored Messaging Server configuration information; includes the location of the main server-configuration information, stored on an LDAP directory server. See configutil for more details.

Table 1.1 Important Messaging Server directories and files (Continued)

Directory or file	Default or required location	Explanation
SMTP routing table	*instanceDirectory*/config/configdb	A portion of the file configdb consisting of routing instructions for forwarding messages from this server to other servers. SeeEditing SMTP Routing Table Entries for more details.
trusted directory	*instanceDirectory*/smtp-bin/delivery (required location)	The directory that holds programs that work with program delivery. See the appendix Program Delivery for more details.
Mailstone utility	/mailstone/ (default location after separate Mailstone installation)	The directory that holds the executable and configuration files for the Mailstone stress-testing utility. See *Netscape Mailstone Utility* for more details.
Messaging Multiplexor	*serverRoot*/mmp/ (default location after separate Multiplexor installation)	The directory that holds the executable and configuration files for Messaging Multiplexor server. See *Netscape Messaging Multiplexor* for more details.
log files	*instanceDirectory*/log/*service* (default location) where *service* is the name of the service (such as IMAP) being logged	The directories containing sets of log files for each of the services provided by Messaging Server. See the chapter Logging and Log Analysis for more details.
SMTP plug-ins configuration file	*instanceDirectory*/smtp-bin/plugins/plugins.cfg (required location)	The file that specifies which SMTP plug-ins have been installed and what their configurations are. See the chapter Working With SMTP Plug-Ins for more details.

Table 1.1 Important Messaging Server directories and files (Continued)

Directory or file	Default or required location	Explanation
UBE filter configuration file	*instanceDirectory*/smtp-bin/plugins/UBEfilter.cfg (default location)	The file that contains the mail filtering rules for the Unsolicited Bulk Email (UBE) plug-in. See the chapter Filtering Unsolicited Bulk Email for more details.
End-user interface HTML pages	*serverRoot*/bin/user/admin/ (default location)	Customizable HTML pages and associated CGIs that provide end-user access to account information. See Configuring End-User Information for more details.

Using Netscape Console

Netscape Console is a Java application that provides server administrators with a graphical interface for managing all Netscape servers. From any installed instance of Netscape Console, you can see and access all the Netscape servers on your enterprise's network to which you have been granted access rights. (See Configuring Administrator Access to Messaging Server for information on how administrator access to servers is configured.) For complete documentation on Netscape Console, see *Managing Servers with Netscape Console*.

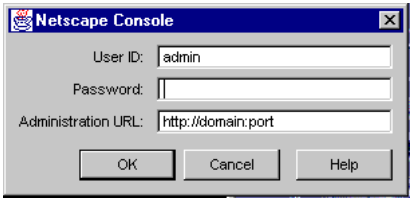
If you need to create a new instance of Netscape Console for managing Messaging Server, use the Netscape Server Setup program (see The Installation Process) to install Netscape Console onto the machine from which you intend to administer your Messaging Servers. You can install Netscape Console onto the same host as a Messaging Server, or onto any other machine on the network.

> **Note:** For any given instance of Netscape Console, the limits of the network it can administer are defined by the set of resources whose configuration information is stored in the same configuration directory. That is the maximum set of hosts and servers that can appear in the Console window.

For a given administrator using Netscape Console, the actual number of visible serves and hosts may be fewer, depending on the access permissions that administrator has.

When you launch Netscape Console, it first displays a login window (Figure 1.9). You enter your administrator's ID, your password, and the URL (including port number) of the Administration Server representing a server group to which you have access. You cannot use Netscape Console without having login access to at least one server group on your network.

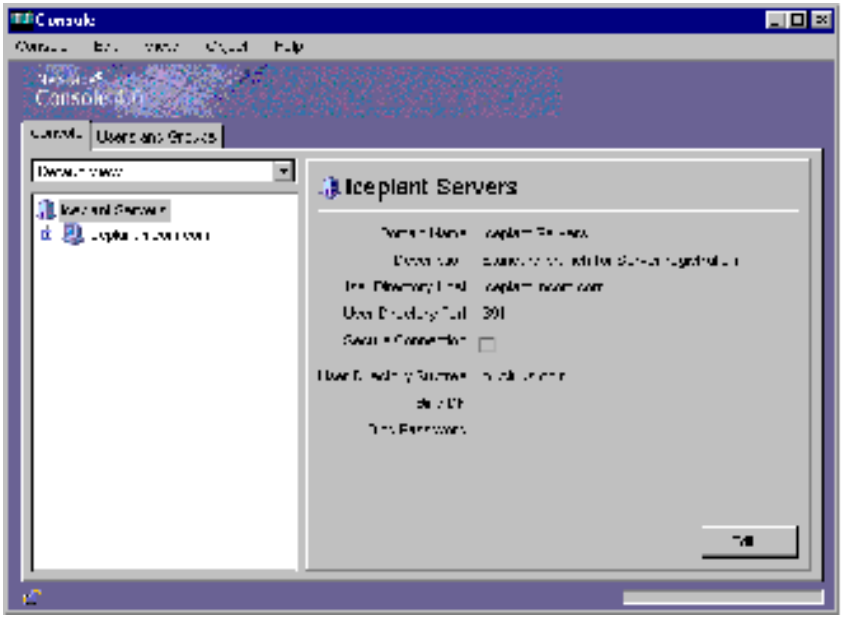
Figure 1.9 Netscape Console login window



If the information you enter into the login window is acceptable, Netscape Console displays a graphical representation of all the hosts and servers on your network that you have access to.

In the example shown in Figure 1.10, the left pane of the Console window shows that the entire network to which the administrator has access consists of a single host machine and all the servers on it. (See *Managing Servers with Netscape Console* for an explanation of the administrative-domain information displayed in the right pane of Figure 1.10.)

Figure 1.10 Netscape Console window (with Domain Information form)

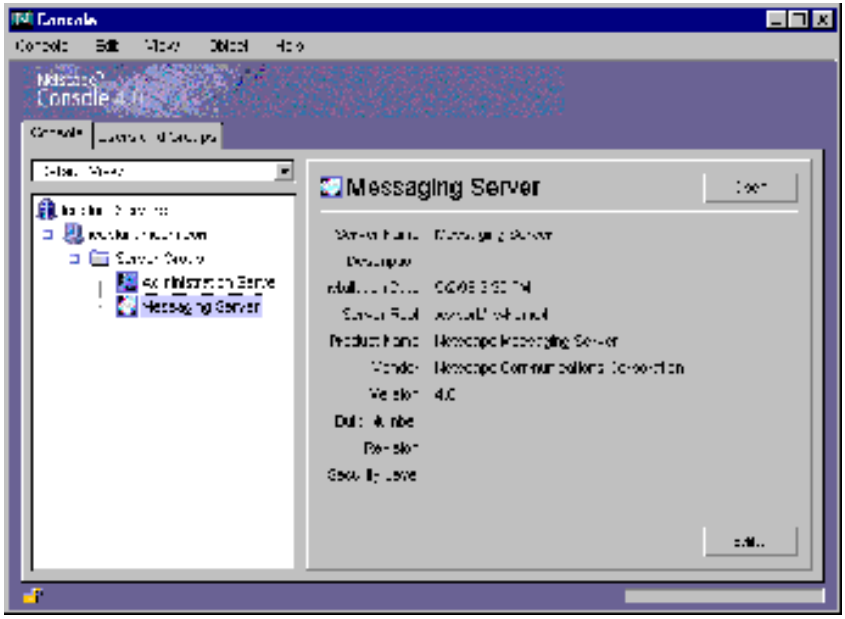


Getting to a Messaging Server

After you have launched Netscape Console, take these steps to access the instance of Messaging Server you want to manage:

1. In the Netscape Console window, click the Console tab if it is not already frontmost.
2. Open the icon of the host machine containing the server.
3. Open the folder icon representing the server group that contains the server.
4. Select the icon of the server itself. The Server Information form for the selected server appears, as shown in Figure 1.11.
5. Open the selected Messaging Server. Either click the Open Server button in the Server Information form or double-click the selected server icon below the Console tab. The Messaging Server Tasks form, described next, appears.

Figure 1.11 Netscape Console window (with Server Information form)



Performing Typical Tasks

When you open Messaging Server from Netscape console, the first item displayed is the Tasks form (Figure 1.12). The Tasks form contains a list of common Messaging Server administration tasks; clicking the button beside a task opens windows through which you can perform the task.

Figure 1.12 Messaging Server Tasks form

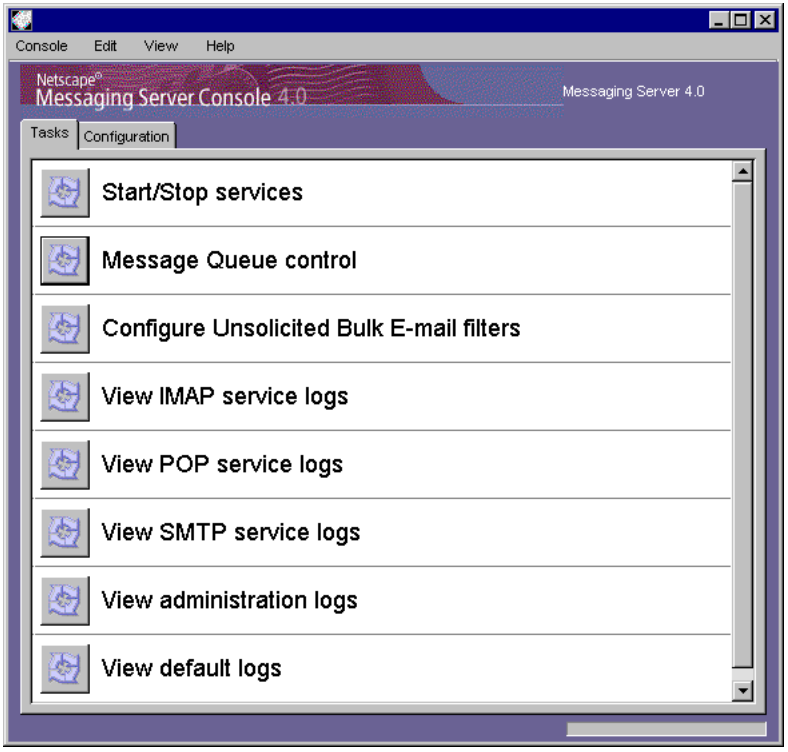


Figure 1.12 shows the full list of available tasks. When you open a Messaging Server, you may see fewer tasks, depending on your access rights to the server. See Configuring Administrator Access to Messaging Server for more information on administrator access to server tasks.

Table 1.2 directs you to the part of this book that describes procedures for performing each task listed in Figure 1.12.

Table 1.2 Documentation for tasks listed in the Tasks form

Task	Where described
Start/Stop services	Starting and Stopping Services
Message Queue control	Managing the Message Queue
Configure Unsolicited Bulk Email filters	Filtering Unsolicited Bulk Email

Table 1.2 Documentation for tasks listed in the Tasks form (Continued)

Task	Where described
View IMAP Service logs	Searching and Viewing Logs
View POP Service logs	Searching and Viewing Logs
View SMTP Service logs	Searching and Viewing Logs
View administration logs	Searching and Viewing Logs
View default logs	Searching and Viewing Logs

Using the Task form is not the only way to access server tasks. If you have the required access rights to the server, you can perform all the tasks shown in Figure 1.12--and many other tasks as well--through the Configuration Tab (described next).

Performing All Configuration and Administration Tasks

You can use the Configuration Tab to access all task and configuration forms available through Netscape Console. Access through the Configuration tab is more complete, though not always as direct, as through the Tasks form. Take these steps to access a task through the Configuration tab:

1. In Netscape Console, open the Messaging Server that you want to configure. (See Getting to a Messaging Server if you need instructions.)

2. Click the Configuration tab.

   The left pane of the window displays a hierarchical set of icons that represent the services and features of Messaging Server. The Messaging Server icon itself is at the top; directly below it are icons for Services, Message Store, and Log files. These icons can be individually selected, and some can also be opened to reveal other icons that can themselves be selected or opened.

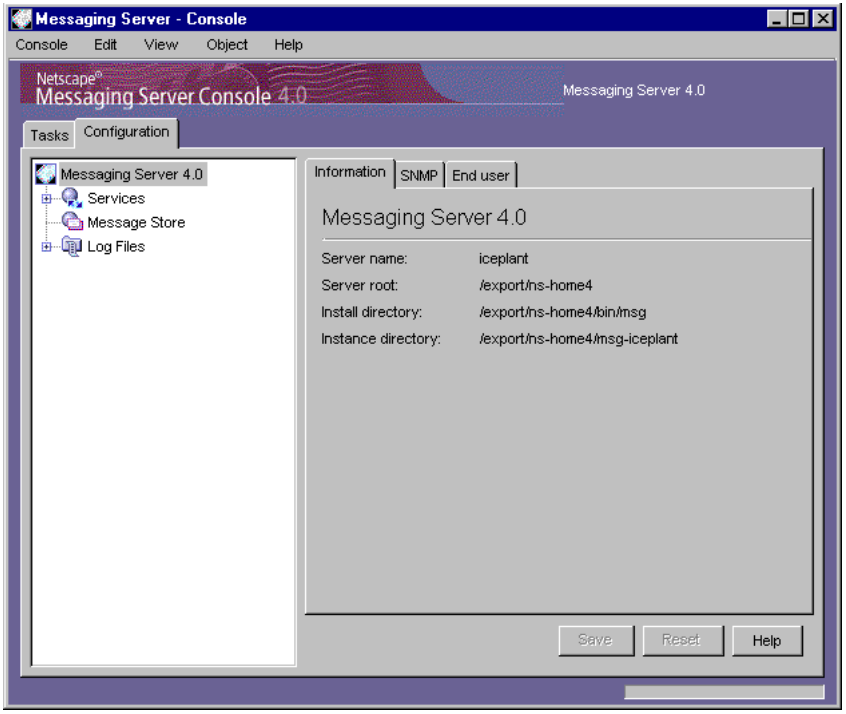
3. Select an icon, or open an icon and select one of the icons that appear below it.

The right pane displays a form, possibly including tabs for accessing additional forms. For forms that include tabs, clicking a tab displays another form related specifically to that tab.The form or forms are the interface to a configuration or administration task represented by the selected icon.

4. View or enter information into the forms, as appropriate, to complete the task.

For example, if you select the Messaging Server icon itself in the left pane, the right pane displays the three tabs shown in Figure 1.13.

Figure 1.13 Messaging Server Configuration form with Messaging Server icon selected



The tasks that you can perform through these Netscape Console forms are described throughout the rest of this book.

Note: The set of tasks available in this manner is a superset of the tasks available through the Tasks form described in the previous section. Also note that some server tasks can be performed from the command line; see Using the Command Line (next).

Using the Command Line

Netscape Messaging provides a set of command-line utilities as an alternative to using the Netscape Console interface for performing certain configuration and administration tasks. In the case of massive or repetitive operations, such as batch processing of user accounts, it can be far more efficient to use the command line than to manually enter information at the console.

Table 1.3 lists the command-line utilities available with Messaging 4.0. For reference information on these utilities, see Appendix A, Command-line Utilities, and Appendix C, sendmail Migration and Compatibility.

Table 1.3 Command-line utilities

Command-line utility	Description
Management	
`configutil`	Lets you view and make changes to server configuration settings (both local settings and settings stored in the configuration directory).
`imscripter`	Executes an IMAP command or sequence of commands.
`mboxutil`	Lists, creates, renames, or moves mailboxes.
`hashdir`	Identifies the directory that contains the message store for a particular user.
`processq`	Manually delivers messages from the mail queue.
`deliver`	Delivers mail to a user mailbox.
`stored`	Performs background and daily tasks on the message store; erases expunged messages.
Monitoring and reporting	
`counterutil`	Monitors a counter object and displays all counters in it.
`mailq`	Checks the mail queue and reports the number of messages in it.
`quota`	Reports mailbox quota usage.
`readership`	Collects readership information on shared mailboxes.

Table 1.3 Command-line utilities (Continued)

Command-line utility	Description
Recovery	
`NscpMsg`	Starts and stops the server and resets configuration variables (Unix only).
`reconstruct`	Reconstructs mailboxes that have been damaged or corrupted.
Migration from another mail server	
`MoveUser`	Moves contents of user mailboxes from one Messaging to another.
`qconvert`	Converts a Messaging 3.x message queue to Messaging 4.0 format.
`upgrade`	Converts Messaging 3.x mailboxes to 4.0 format and moves them to the 4.0 server.
Migration from `sendmail`	
`unix2ldif`	Converts Unix `sendmail` user-account information to LDAP Directory Interchange Format (LDIF).
`ldifsplit`	Analyzes the results of the `ldifsplit` utility, separating the LDIF data into entries that are already in the user directory from those that are not.
`chkuniq`	Checks the output of `unix2ldif` and `ldifsplit` for duplicate entries.
`ldapmodify`	Updates an LDAP directory with the LDIF output of the `sendmail` utilities.
`MigrateUnixSpool`	Moves user messages from `sendmail` spool files to Messaging Server mailboxes.

Other command-line utilities described in the appendix include those for managing the Messaging Multiplexor server, described in *Netscape Messaging Multiplexor,* and the Mailstone stress-testing utility, described in *Netscape Mailstone Utility*.

In this book, the description of each server task you can perform includes a discussion of the command-line utilities, if any, that you can use to accomplish the task.

Configuring General Messaging Capabilities

This section describes the general Messaging Server tasks--such as starting and stopping services, configuring directory access, and configuring end-user access--that you can perform with Netscape Console or with command-line utilities. Tasks specific to individual Messaging Server services--such as POP, IMAP, and SMTP--are described in subsequent chapters.

Viewing Basic Server Information

You can review some of the basic information about an installed Messaging Server by viewing its Information form in Netscape Console.

To display the Information form:

1. In Netscape Console, open the Messaging Server whose information you want to view.
2. Select the server's icon in the left pane.
3. Click the Information tab in the right pane, if it is not already frontmost.

   The Information form appears. It displays the server name, server root directory, installation directory, and instance directory. (See Table 1.1 for an explanation of these terms.)

See Server Information Tab for a complete description of the contents of this form.

SNMP Setup

You can use Netscape Console to set up and enable the Simple Network Management Protocol (SNMP) subagent for your Messaging Server. By using SNMP, an administrator can monitor multiple servers remotely through an SNMP network management station.

The Messaging Server subagent collects information and generates statistics relating to the server's functioning, and it transfers the information to the SNMP master agent.

Although this task is a general configuration task, it is described in Chapter 10, Monitoring and Maintaining Your Server. For a description of the Messaging Server SNMP management information base, see Appendix D, SNMP MIB. For information on setting up your network's SNMP master agent, see *Managing Servers with Netscape Console.*

Configuring End-User Information

Messaging Server provides end users with limited server access, through which they can manage certain aspects of their own mail accounts and also create or subscribe to mailing lists. The server employs HTML forms that users fill out to make these changes.

Messaging Server 4.0 includes a set of HTML forms (and associated CGI scripts) for this purpose. As server administrator, you can control which forms, if any, users can access, and where those forms are located. You specify the URLs to those forms, so that client software that connects to your server can access the forms. The following forms are provided with Messaging Server:

- **Personal Account Manager.** This form allows users to perform tasks such as changing their passwords or modifying their personal information (home phone number, vacation message, and so on).
- **Mail Account Manager.** This form allows users to manage parts of their mail-account configuration, including changing the access permissions for their own mail folders so that they can share folders with other users.

You can use the provided forms unchanged, or you can customize them for your enterprise. Note that the forms are complex; making more than minor cosmetic changes (especially to the Mail Account Manager form) can be a difficult process, requiring sophisticated manipulation of HTML and JavaScript. Whether you customize them or not, you should leave the forms in their default locations (`serverRoot/bin/user/admin/html/`) on the server.

On the other hand, if you have already implemented end-user access to directory information with HTML forms of your own design, you can provide client access to those forms by using Netscape Console to specify their URLs.

In addition to controlling access to end-user forms, Messaging Server also allows you to create a greeting message to be sent to each new user.

To configure end-user access or create a new-user greeting:

1. Generate the HTML forms you need, or modify and use the forms provided with Messaging Server 4.0.
2. Store the forms in an appropriate location. The default location for the forms provided with Messaging Server 4.0 is *serverRoot*/bin/user/admin/html/.
1. In Netscape Console, open the Messaging Server whose end-user access you want to configure.
2. Click the Configuration tab. If the server's icon in the left pane is not already highlighted, select it.
3. Click the "End user" tab in the right pane. The End User Configuration form appears.
4. Make changes to the form URLs as needed. The default URLs are consistent with the default locations of the HTML files.
5. Create a new-user greeting or make changes, as needed.

   You must format the greeting as an email message, with a header (containing at least a subject line), then a blank line, then the message body.

   When you create a message, specify its language with the popup menu above the message field. You can create several messages in several languages, if desired. If you do, the locale of each new user is compared to the language of the message, and the server sends the correct message to the new user.
6. Click Save.

See End-User Configuration Tab for a complete description of the contents of this form.

Starting and Stopping Services

Netscape Console provides a form that allows you to start and stop individual services and view status information about each of them.

For each service--IMAP, POP, and SMTP--the form displays the service's current state (on or off). If the service is running, the form shows the time at which the service was last started up, and it can also display other status information.

> **Note:** You must first enable the POP and IMAP services before starting or stopping them. See Enabling and Disabling IMAP and POP.

You need to run only the services that your server actually uses. For example, if you are temporarily using a particular instance of Messaging Server solely as a message transfer agent (MTA), you can turn on SMTP alone. Or, if maintenance, repair, or security needs require shutting down the server, you may be able to turn off just the affected service. (If you never intend to run a particular service, you should disable it instead of just turning it off.)

To start up, shut down, or view the status of any messaging services:

1. From Netscape Console, open the Messaging Server whose services you want to start or stop.

2. Get to the Services General Configuration form in either of these two ways:

   - Click the Tasks tab, then click "Start/Stop Services".

   - Click the Configuration tab and select the Services folder in the left pane. Then select the General tab in the right pane.

3. The Services General Configuration form appears.

   The left column of the Process Control field lists the services supported by the server; the right column gives the basic status of each of the services (ON or OFF, plus--if it is ON--the time it was last started).

4. To view status information about a service that is currently on, select the service in the Process Control field. The Service Status field displays status information about the service.

   For POP and IMAP, the field shows the last connection time, the total number of connections, the current number of connections, the number of failed connections since the service last started, and the number of failed logins since the service last started.

   For SMTP, the field shows the current number of queued messages, the total number of messages sent and received since startup, and the current numbers of messages waiting for both external and internal delivery.

The information in this field helps you to understand the load on the server and the reliability of its service, and it can help spotlight attacks against the server's security.

5. To turn a service on, select it in the Process Control field and click Start.

6. To turn a service off, select it in the Process Control field and click Stop.

7. To turn all enabled services on or off simultaneously, click the Start All or Stop All button.

See Services General Configuration Tab for a complete description of this form's contents.

Command-line utility. On Unix platforms you can also use the `NscpMsg` utility to start or stop any of the messaging services. See `NscpMsg` for more information.

Customizing Directory Lookups

Netscape Messaging Server 4.0 cannot function without an LDAP-based directory system such as the Netscape Directory Server. Messaging Server and Netscape Console require directory access for three purposes:

- When you first install a Messaging Server, you enter configuration settings for the server. These settings are stored in a central *configuration directory*. Part of the installation process includes configuring the connection to that directory.

- When you create or update account information for mail users or mail groups, you enter that information through the Users and Groups interface of Netscape Console. The information is stored in a directory called the *user directory*. Your server group's Administration Server is configured at installation so that when you access Users and Groups, Netscape Console connects by default to the user directory that defines your *administrative domain*--the set of Netscape servers that all share the same configuration directory and user directory.

- When routing messages and delivering mail to mailboxes, Messaging Server looks up information about the sender or recipient(s) in the user directory. By default, Messaging Server looks in the same user directory that its Administration Server has been configured to use.

You can modify each of these directory-configuration settings in the following ways:

- The Administration Server interface of Netscape Console lets you change the connection settings for the configuration directory. (See the Administration Server chapter of *Managing Servers with Netscape Console* for more information.)
- The Users and Groups interface of Netscape Console lets you temporarily connect to a different user directory from the default when making changes to user and group information. (See the Users and Groups chapter of *Managing Servers with Netscape Console* for more information.)
- The Messaging Server interface of Netscape Console lets you configure your Messaging Server to connect to a different user directory from the default defined by the Administration Server. This is the configuration task discussed in this section.

Reconfiguring your Messaging Server to connect to a different user directory for user and group lookups is strictly optional. In most cases, the user directory that defines your server's administrative domain is the one used by all servers in the domain.

> **Important:** If you specify a custom user directory for your Messaging Server lookups, you must also specify that same directory whenever you access the Users and Groups interface of Netscape Console to make changes to the directory's user or group information. See Chapter 4, Managing Mail Users and Mailing Lists, for more information.

To modify the Messaging Server LDAP user-lookup settings:

1. From Netscape Console, open the Messaging Server whose LDAP connection you want to customize.
2. Click the Configuration tab.
3. Select the Services folder in the left pane.
4. Select the LDAP tab in the right pane. The LDAP form appears.

The LDAP form displays the configuration settings for both the configuration directory and the user directory. The configuration-directory settings, however, are read-only in this form. See the Administration Server chapter of *Managing Servers with Netscape Console* if you need to change them.

5. To change the user-directory connection settings, click the box labeled "Use messaging server specific directory settings".

6. Update the LDAP configuration by entering or modifying any of the following information (for explanations of directory concepts, including definitions of terms such as *distinguished name,* see the *Directory Server Administrator's Guide*):

   Host name: The name of the host machine on which the directory containing your installation's user information resides. This is typically not the same as the Messaging Server host, although for very small installations it might be.

   Port number: The port number on the directory host that Messaging Server must use to access the directory for user lookup. This number is defined by the directory administrator, and may not necessarily be the default port number (389).

   Bind DN: The distinguished name that your Messaging Server uses to represent itself when it connects to the directory server for lookups. The bind DN must be the distinguished name of an entry in the user directory itself that has been given search privileges to the user portion of the directory. If the directory allows anonymous search access, you can leave this entry blank.

   Base DN: The search base--the distinguished name of a directory entry that represents the starting point for user lookups. To speed the lookup process, the search base should be as close as possible in the directory tree to the information being sought. If your installation's directory tree has a "people" or "users" branch, that is a reasonable starting point.

7. To change the password used, in conjunction with the Bind DN, to authenticate this Messaging Server to the LDAP directory for user lookups, click the Change password button. A Password-Entry window opens, into which you can enter the updated password.

Your own security policies should determine what password you use in this situation. Initially, the password is set to no password. The password is not used if you have specified anonymous access by leaving the Bind DN field blank.

To return to using the default user directory, uncheck the "Use messaging server specific directory settings" box.

See LDAP Configuration Tab for a complete description of the contents of that form. See Password Entry Window for a complete description of the contents of that window.

Encryption Settings

You can use Netscape Console to enable Secure Sockets layer (SSL) encryption and authentication for Messaging Server and to select the specific encryption ciphers that the server will support across all of its services.

Although this task is a general configuration task, it is described in Enabling SSL. That section is part of Chapter 6, Security and Access Control, which also contains background information on all security and access-control topics for Messaging Server.

Where to Go from Here

This chapter has provided background information on messaging deployment and Messaging Server installation, and it has described how to make general configuration settings to Messaging Server. Subsequent chapters in this book describe the bulk of the administrative tasks, from configuring services through setting up users and groups to monitoring and maintaining the server.

To perform the following tasks, go to the chapters or appendixes indicated.

- **To configure services:**
  - Chapter 2, Configuring IMAP and POP Services
  - Chapter 3, Configuring SMTP Services
  - Chapter 5, Managing the Message Store

- Chapter 6, Security and Access Control
- Chapter 9, Message Routing
- Appendix B, Program Delivery
- Appendix A, Command-line Utilities
- *Netscape Messaging Multiplexor*

- **To set up mail users and mailing lists:**
  - Chapter 4, Managing Mail Users and Mailing Lists
  - Appendix C, sendmail Migration and Compatibility
- **To work with plug-ins and UBE filters:**
  - Chapter 7, Working With SMTP Plug-Ins
  - Chapter 8, Filtering Unsolicited Bulk Email
- **To monitor and maintain the server:**
  - Chapter 10, Monitoring and Maintaining Your Server
  - Chapter 11, Logging and Log Analysis
  - Appendix D, SNMP MIB
  - *Netscape Mailstone Utility*

Interface Reference: General Messaging Services

This section describes the Netscape Console interface elements that allow you to execute and perform general configuration of the services supported by Messaging Server. See *Managing Servers with Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

Messaging Server Tasks Tab

You use the form accessed through this tab as a convenient way to quickly perform several typical Messaging Server administration tasks. The Tasks form provides direct access to common tasks that may be less directly accessible through the Configuration tab.

For more information, see also Performing Typical Tasks.

The Tasks form contains the following elements:

Start/Stop services. Click this button to display a window (see Services General Configuration Tab) that allows you to start or stop any of the Messaging Server services.

Message Queue control. Click this button to display a form (see Queued Messages Tab) that allows you to manage the Messaging Server message queues.

Configure Unsolicited Bulk Email filters. Click this button to display a form (see Unsolicited Bulk Email Configuration Tab) that allows you to create or modify filters that can help block unwanted email.

View IMAP service logs. Click this button to display a form (see Log Files Content Tab) from which you can select, view, and search the contents of an IMAP log file.

View POP service logs. Click this button to display a form (see Log Files Content Tab) from which you can select, view, and search the contents of a POP log file.

View SMTP service logs. Click this button to display a form (see Log Files Content Tab) from which you can select, view, and search the contents of an SMTP log file.

View administration logs. Click this button to display a form (see Log Files Content Tab) from which you can select, view, and search the contents of a Messaging Server administration log file.

View default logs. Click this button to display a form (see Log Files Content Tab) from which you can select, view, and search the contents of a log file created by a Messaging Server service or utility other than one listed above.

Messaging Server Configuration Tab

You use the form accessed through this tab to get to and configure all the services, as well as the message store and log files, of Messaging Server. You can perform all administration tasks from the Configuration form.

For more information, see also Performing All Configuration and Administration Tasks.

In the left pane of the Configuration form, you can select and open any of the icons (Services, Message Store, or Log Files) to gain further access to Messaging Server components.

The right pane contains three tabs. For descriptions of the forms accessed through these tabs, see the following sections:

- Server Information Tab
- SNMP Tab
- End-User Configuration Tab

Server Information Tab

You use the form accessed through this tab to view basic, read-only configuration information about Messaging Server.

For more information, see also Viewing Basic Server Information.

The Information form has the following non-editable fields:

Server name. The name given to this instance of Messaging Server when it was installed.

Server root. The directory that holds all of this server's files, plus the files of its Administration Server, plus the files of any other Netscape servers in the same server group (that is, administered by that Administration Server). A host typically has only one server root, but more than one is possible, especially if different version numbers of the same server are installed on a single host.

Install directory. The directory, within the server root directory, that holds all of the Messaging Server executable program files.There can be only one Messaging Server installation directory within the server root.

Instance directory. The directory, within the server root directory, that holds the files that define this instance of Messaging Server plus the files created and maintained by this instance. There may be multiple Messaging Server instance directories within the server root.

Action Buttons

Help. Click this button to display online help (this document) that describes the Information form.

End-User Configuration Tab

You use the form accessed through this tab to configure end-user access to account-management forms and to specify a greeting message sent to new users.

For more information, see also Configuring End-User Information.

The End-User Configuration form has the following elements:

Personal Account Manager URL. In this field, enter the URL to the form that allows users to manage their personal information.

Mail Account Manager URL. In this field, enter the URL to the form that allows users to manage mail-account configuration, including sharing access to their mail folders.

New user greeting form. In this field, enter the text of the greeting that is to be sent to each new user. Format the greeting as an email message, with a header (containing at least a subject line), then a blank line, then the message body. You can create different messages in different languages; use the popup menu above the field to specify the language of each greeting message that you create. The appropriate message is then sent to each new user whose locale corresponds to one of the languages you select.

Action Buttons

Save. Click this button to commit any settings you have made in the End-User Configuration form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the End-User Configuration form.

Services General Configuration Tab

You use the form accessed through this tab to start, stop or view the status of any services of the Messaging Server.

For more information, see also Starting and Stopping Services.

The Services General Configuration form has the following elements:

Process Control. This field lists all accessible Messaging Server services (in the Service column) and their fundamental status (in the ON/OFF column).

Service. This column of the Process Control field lists all the Messaging Server services that you can start or stop. These are the available services:

IMAP
POP
SMTP

If you select a service in the Process Control field, you can then apply the Start or Stop buttons to it.

ON/OFF. This column of the Process Control field notes, for each service listed in the Service column, whether the service is off or on, and (if on) when it was last started.

Start. Click this button to start a service that you have selected in the Service field.

Stop. Click this button to stop a service that you have selected in the Service field.

Start All. Click this button to start all services.

Stop All. Click this button to stop all services.

Service status. This field displays the status of the service currently selected in the Services column. (The field is blank for inactive services.) These are items displayed in the field for the POP or IMAP service:

Last connection time. The time at which the most recent connection was made to this service. This can tell you, for example, whether the server is having problems accepting connections.

Total number of connections. The number of connections that have been made to this service since it was last started. This can give you an overall, time-averaged picture of the level of this service's activity.

Number of current connections. The number of currently active connections to this service. This can give you an idea of how heavily loaded the server currently is.

Number of failed connections. The number of connection requests that have been refused since the service last started. This can spotlight network problems or indicate an overloaded server.

Number of failed logins. The number of login requests that have been refused by the service since it last started. This can help spotlight attacks against the security of the server.

These are items displayed in the field for the SMTP service:

Number of messages stored. The current total (physical) number of queued messages.

Number of messages sent. The total number of messages sent through SMTP-Deliver since startup.

Number of messages received. The total number of messages accepted through SMTP-Accept since startup.

Outgoing queued messages. The current total (logical) number of queued messages waiting to be sent to another MTA.

Incoming queued messages. The current total (logical) number of queued messages waiting to be delivered locally.

Action Buttons

Help. Click this button to display online help (this document) that describes the Services General Configuration form.

LDAP Configuration Tab

You use the form accessed through this tab to view and configure connections to the LDAP directory used by your Messaging Server.

For more information, see also

- Customizing Directory Lookups
- *Installing Messaging Server 4.0* (for setting configuration-directory parameters)

The LDAP form has the following elements:

LDAP Connection for Server Configuration

Host name. A non-editable field that lists the host name of the LDAP directory server on which the configuration information for this Messaging Server is stored.

Port number. A non-editable field that lists the port number to be used for access to the LDAP directory server on which the configuration information for this Messaging Server is stored.

Bind DN. A non-editable field that lists the bind distinguished name, the user name under which this Messaging Server accesses the LDAP directory server on which its configuration information is stored.

Base DN. A non-editable field that lists the search base, the distinguished name of the location in the LDAP directory at which to start searching for the configuration information for this Messaging Server.

LDAP Connection for User Lookup

Use Messaging Server-specific directory settings. Check this box if you want to customize the LDAP connection for user lookup by changing any of the following fields: Host name, Port number, Bind DN, Base DN. Uncheck this box to return to using the default user directory for your server group.

Host name. Use this field to specify the host name of the LDAP directory server on which this Messaging Server is to look up user and group information.

Port number. Use this field to specify the port number used to access the LDAP directory server on which this Messaging Server is to look up user and group information.

Bind DN. Use this field to specify the bind distinguished name, the user name under which this Messaging Server accesses the LDAP directory server to obtain user and group information.

Base DN. Use this field to specify the search base, the distinguished name of the location in the LDAP directory at which to start searching for user and group information.

Change password. Click this button to open a window (see Password Entry Window) that allows you to change the password to be used to authenticate this Messaging Server to the LDAP directory for user lookups.

Action Buttons

Save. Click this button to commit any settings you have made in the LDAP Configuration form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the LDAP Configuration form.

Password Entry Window

You use this window to change the password that Messaging Server uses to authenticate itself to the LDAP directory for user and group lookup.

For more information, see also Customizing Directory Lookups.

The Password-Entry window has the following elements:

Password. Enter the password in this field.

Confirm password. Re-enter the password in this field. If what you enter is different from what you entered in the Password field, you are prompted to try again.

Action Buttons

OK. Click this button to commit to the changed password and close the Password-Entry window.

Cancel. Click this button to cancel the password-changing operation and close the Password-Entry window, leaving the current password unchanged.

Help. Click this button to display online help (this document) that describes the Password-Entry window.

Chapter

2

Configuring IMAP and POP Services

Netscape Messaging Server 4.0 supports both the Internet Mail Access Protocol 4 (IMAP4) and the Post Office Protocol 3 (POP3) for client access to mailboxes. IMAP and POP are both Internet-standard mailbox protocols. This chapter describes how to use Netscape Console to configure your server to support either or both of these services. For information on configuring Simple Mail Transfer Protocol (SMTP) services, see Chapter 3, Configuring SMTP Services.

You can also perform many IMAP and POP configuration tasks through the command-line utility `configutil`. That process is not described here; see Appendix A, Command-line Utilities, for instructions.

This chapter does not discuss how to configure client access controls for IMAP or POP; see Chapter 6, Security and Access Control, for information on that topic.

This chapter has the following sections:

- General Configuration
- Login Requirements
- Performance Parameters
- Client Access Controls
- Configuring IMAP and POP with Netscape Console
- Interface Reference: IMAP and POP Configuration

General Configuration

Configuring the general features of the Messaging Server IMAP and POP services includes enabling or disabling IMAP or POP service, assigning port numbers, and optionally modifying service banners sent to connecting clients. This section provides background information; see Configuring IMAP and POP with Netscape Console for the steps you follow to make these settings.

Enabling and Disabling IMAP and POP

You can control whether any particular instance of Messaging Server makes its IMAP or POP service available for use. This is not the same as turning IMAP or POP on or off (see Starting and Stopping Services); to function, IMAP or POP must be both enabled and turned on.

Enabling is a more "global" process than turning on or off. For example, the Enable setting persists across system reboots, whereas you must restart a previously "on" service after a reboot.

There is no need to enable services that you do not plan to use. For example, if a Messaging Server instance is used only as a message transfer agent (MTA), you should disable both POP and IMAP. If it is used only as a POP post office, you should disable IMAP.

IMAP and POP Port Numbers

If you enable the IMAP service, you can specify the port number that the server is to use for IMAP connections. The default is 143.

Likewise, if you enable the POP service, you can specify the port number that the server is to use for POP connections. The default is 110.

You might need to specify a port number other than the default if you have, for example, two or more IMAP server instances on a single host machine, or if you are using the same host machine as both an IMAP server and a Messaging Multiplexor server. (See the document *Netscape Messaging Multiplexor* for information about the Multiplexor.)

Keep the following in mind when you specify a port:

- Port numbers can be any number from 1 to 65535.
- Make sure the port you choose isn't already in use or reserved for another service.

Port for IMAP over SSL

Messaging Server supports encrypted communications with IMAP and POP clients by using the Secure Sockets Layer (SSL) protocol. See Configuring SSL Encryption and Authentication for general information on support for SSL in Messaging Server.

You can accept the default IMAP over SSL port number (993) or you can specify a separate port for IMAP over SSL.

Messaging Server provides the option of using separate ports for IMAP and IMAP over SSL because most current IMAP clients require separate ports for them. Same-port communication with both IMAP and IMAP over SSL is an emerging standard; as long as your Messaging Server has an installed SSL certificate (see Obtaining Certificates), it can support same-port IMAP over SSL.

> **Note:** Messaging Server 4.0 supports POP over SSL, but not through a separate port from POP. In any case, some client software (such as the current release of Netscape Messenger, the Netscape mail client) does not support POP over SSL.

Service Banner

When a client first connects to the Messaging Server IMAP or POP port, the server sends an identifying text string to the client. This service banner (not normally displayed to the client's user) identifies the server as Netscape Messaging Server, gives the server's version number, and notes the time of connection. The banner is most typically used for client debugging or problem-isolation purposes.

You can replace the default banner for the IMAP or POP service if you want a different message sent to connecting clients.

Login Requirements

You can control how users are permitted to log in to the IMAP or POP service to retrieve mail. You can allow anonymous login (for IMAP only), password-based login, and certificate-based login. This section provides background information; see Configuring IMAP and POP with Netscape Console for the steps you follow to make these settings.

Anonymous Login

Anonymous login refers to a user logging in under the special user name `anonymous`, which requires no password. (By convention analogous to that of FTP, users enter their email addresses as passwords, so that their accesses are logged.) One reason for permitting anonymous login might be to provide read-only access to, for example, archived messages of a mailing list.

By default, anonymous login for IMAP is disabled. Anonymous login is not available for the POP service.

Password-Based Login

In typical messaging installations, users access their IMAP or POP mailboxes by entering a password into their mail client. The client sends the password to the server, which uses it to authenticate the user. If the user is authenticated, the server decides, based on access-control rules, whether or not to grant the user access to certain mailboxes stored on that server.

If you allow password login, users can access IMAP or POP by entering a password. Passwords are stored in an LDAP directory and can be either clear text or encrypted. Directory policies determine what password policies, such as minimum length, are in effect.

If you disallow password login, password-based authentication is not permitted. Users are then required to use certificate-based login, as described in the next section.

To increase the security of password transmission when you have selected password-based login, you can specify that passwords be encrypted before they are sent to your server. You do this by selecting a minimum cipher-length requirement for login.

- If you choose 0, you do not require encryption. Passwords are sent in the clear or they are encrypted, depending on client policy.
- If you choose a nonzero value, the client must establish an SSL session with the server--using a cipher whose key length is at least the value you specify--thus encrypting any IMAP or POP user passwords the client sends.

If the client is configured to require encryption with key lengths greater than the maximum your server supports, or if your server is configured to require encryption with key lengths greater than what the client supports, password-based login cannot occur. See Enabling SSL for information on setting up your server to support various ciphers and key lengths.

Certificate-Based Login

In addition to password-based authentication, Netscape servers support the authentication of users through examination of their digital certificates. Instead of presenting a password, the client presents the user's certificate when it establishes an SSL session with the server. If the certificate is validated, the user is considered authenticated.

For instructions on setting up Messaging Server to accept certificate-based user login to the IMAP service, see Setting Up Certificate-Based Login.

You don't need to uncheck the "Allow plaintext-password login" box in the IMAP System form to enable certificate-based login. If the box is checked (its default state), and if you have performed the tasks required to set up certificate-based login, both password-based and certificate-based login are supported. Then, if the client establishes an SSL session and supplies a certificate, certificate-based login is used. If the client does not use SSL or does not present a client certificate, the server requests a password.

Performance Parameters

You can set some of the basic performance parameters for the IMAP and POP services of Messaging Server. Based on your hardware capacity and your user base, you can adjust these parameters for maximum efficiency of service. This section provides background information; see Configuring IMAP and POP with Netscape Console for the steps you follow to make these settings.

Number of Processes

Messaging Server can divide its work among several executing processes, which in some cases can increase efficiency. This capability is especially useful with multiprocessor server machines, in which adjusting the number of server processes can allow more efficient distribution of multiple tasks among the hardware processors.

There is a performance overhead, however, in allocating tasks among multiple processes and in switching from one process to another. The advantage of having multiple processes diminishes with each new one added. A simple rule of thumb for most configurations is to have one process per hardware processor on your server machine, up to a maximum of perhaps 4 processes. Your optimum configuration may be different; this rule of thumb is meant only as a starting point for your own analyses.

> **Note:** On some platforms you might also want to increase the number of processes to get around certain per-process limits (such as the maximum number of file descriptors), specific to that platform, that may affect performance.

The default number of processes is 1 for both IMAP and POP.

Number of Connections per Process

The more simultaneous client connections your IMAP or POP service can maintain, the better it is for clients. If clients are denied service because no connections are available, they must then wait until another client disconnects.

On the other hand, each open connection consumes memory resources and makes demands on the I/O subsystem of your server machine, so there is a practical limit to the number of simultaneous sessions you can expect the server to support. (You might be able to increase that limit by increasing server memory or I/O capacity.)

IMAP and POP have different needs in this regard:

- IMAP connections are generally long-lived compared to POP connections. When a user connects to IMAP to download messages, the connection is usually maintained until the user quits or the connection times out. By contrast, a POP connection is usually closed as soon as the requested mail has been downloaded.

- IMAP connections are generally very efficient compared to POP connections. Each reconnection during a POP session requires re-authentication of the user, whereas an IMAP connection requires only a single authentication because the connection remains open. POP connections, therefore, involve much greater performance overhead than IMAP connections. Netscape Messaging Server, in particular, has been designed to require very low overhead by open but idle IMAP connections.

Thus, at a given moment for a given user demand, Messaging Server may be able to support many more open IMAP connections than POP connections.

The default value for IMAP is 4000 sessions per process; the default value for POP is 600. These values represent roughly equivalent demands that can be handled by a typically configured server machine. Your optimum configuration may be different; these defaults are meant only as general guidelines.

Number of Threads per Process

Besides supporting multiple processes, Messaging Server further improves performance by subdividing its work among multiple threads. The server's use of threads greatly increases execution efficiency, because commands in progress are not holding up the execution of other commands.

Threads are created and destroyed, as needed during execution, up to the maximum number you have set.

Having more simultaneously executing threads means that more client requests can be handled without delay, so that a greater number of clients can be serviced quickly. However, there is a performance overhead to dispatching among threads, so there is a practical limit to the number of threads the server can make use of.

For both IMAP and POP, the default maximum value is 1000 threads per process. (The numbers are equal despite the fact that the default number of connections for IMAP is greater than for POP. It is assumed that the more numerous, but more often idle, IMAP connections can be handled efficiently with the same maximum number of threads as the fewer, but busier, POP connections.)Your optimum configuration may be different, but these defaults are high enough that it is unlikely you would ever need to increase them; the defaults should provide reasonable performance for most installations.

Dropping Idle Clients

To reclaim system resources used by connections from unresponsive clients, both the IMAP4 and POP3 protocols provide for the server to unilaterally drop connections that have been idle for a certain amount of time.

The default times (10 minutes for POP, 30 minutes for IMAP) are the minimum times that idle connections must remain open, according to the respective protocol specifications. You can increase the idle times beyond the default values, but you cannot make them less.

Idle POP connections are usually caused by some problem (such as a crash or hang) that makes the client unresponsive. Idle IMAP connections, on the other hand, are a normal occurrence. To keep IMAP users from being disconnected unilaterally, IMAP clients typically send a command to the IMAP server at some regular interval that is less than 30 minutes.

Client Access Controls

Netscape Messaging Server includes access-control features that allow you to determine which clients can gain access to its IMAP or POP messaging services (and SMTP as well). You can create flexible access filters that can allow or deny access to clients based on a variety of criteria.

Client access control is an important security feature of Netscape Messaging Server. For information on creating client access-control filters and examples of their use, see Configuring Client Access to TCP Services.

Configuring IMAP and POP with Netscape Console

You can perform basic configuration of the Messaging Server IMAP and POP services through Netscape Console. To configure your IMAP or POP service, take these steps (to configure both IMAP and POP, you need to follow this process twice):

1. From Netscape Console, open the Messaging Server you want to configure.
2. Click the Configuration tab and open the Services folder in the left pane.
3. Select IMAP or POP.
4. Select the System tab in the right pane.
5. Make general configuration settings:
   - Enable or disable the service: see Enabling and Disabling IMAP and POP.
   - Assign port numbers: see IMAP and POP Port Numbers and Port for IMAP over SSL (for IMAP only).
   - If desired, customize the service banner: see Service Banner.
6. Set login requirements:
   - If desired, enable anonymous login: see Anonymous Login (for IMAP only).
   - If desired, enable password-based login: see Password-Based Login.
   - If desired, enable certificate-based login: see Certificate-Based Login.
7. Set performance parameters:
   - Set the number of processes: see Number of Processes.
   - Set the number of connections: seeNumber of Connections per Process.
   - Set the number of threads: see Number of Threads per Process.

- Set maximum idle time: see Dropping Idle Clients.

See IMAP System Tab or POP System Tab for detailed information on the contents of those forms.

Interface Reference: IMAP and POP Configuration

This section describes the Netscape Console interface elements that allow you to configure and execute the Messaging Server IMAP and POP services. See *Managing Servers With Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

IMAP System Tab

You use the form accessed through this tab to set basic configuration parameters for the Messaging Server IMAP service.

For more information, see also

- Configuring IMAP and POP with Netscape Console
- General Configuration
- Login Requirements
- Performance Parameters

The IMAP System form has these elements:

Enable IMAP service at port. Check this box to enable the IMAP service; use the field to enter the number of the port this server will use for IMAP. (Default = 143.

Use separate port for IMAP over SSL. Check this box to enable IMAP over SSL; use the field to enter the number of the port this server will use for IMAP over SSL. (Default = 993, the standard port number for IMAP over SSL).

Allow anonymous login. Check this box to allow users to log in to the IMAP service without using a password, under the name `anonymous`. (Default = not enabled.) The state of the "Allow password login" checkbox has no effect on anonymous login.

Allow password login. Check this box to allow users to log in to the IMAP service by supplying a user name and password. (Default = enabled.)

If this box is checked, you can specify password-encryption requirements in the following field. If this box is not checked, certificate-based login to IMAP is required.

Minimum cipher length for password encryption. Use this field to select the minimum length of encryption cipher that the server will accept for transmission of IMAP passwords. (Default = 0.) A length of 0 means that no encryption is required; passwords can be sent in the clear.

IMAP service banner. (Optional). Use this field to enter a replacement banner for the default IMAP banner that is sent to an IMAP clients when it first connects to the IMAP port. (The default banner identifies the server version and the time of connection.)

Connection Settings

Maximum network sessions. Use this field to specify how many simultaneous IMAP sessions this server is permitted to maintain per process. (Default = 4000.)

Drop client if idle for. Use this field to specify how long (in seconds, minutes, or hours) an idle IMAP connection to a client can remain open before the server drops the connection. (Default = 30 minutes.)

Process Settings

Maximum number of threads per process. Use this field to specify the maximum number of threads the IMAP service is permitted to execute at a time. (Default = 1000.)

Number of processes. Use this field to specify the maximum number of processes that the IMAP service can employ. (Default = 1.)

Action Buttons

Save. Click this button to commit any settings you have made in the IMAP System form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the IMAP System form.

POP System Tab

You use the form accessed through this tab to set basic configuration parameters for the Messaging Server POP service.

For more information, see also

- Configuring IMAP and POP with Netscape Console
- General Configuration
- Login Requirements
- Performance Parameters

The POP System form has these elements:

Enable POP service at port. Check this box to enable POP service; use the field to enter the number of the port this server will use for POP. (Default = 110.)

Allow password login. Check this box to allow users to log into the POP service by supplying a user name and password. (Default = enabled.)

If this box is checked, you can specify password-encryption requirements in the following field. If this box is not checked, certificate-based login to POP is required.

Minimum cipher length for password encryption. Use this field to select the minimum length of encryption cipher that the server will accept for transmission of POP passwords. (Default = 0.) A length of 0 means that no encryption is used; passwords are sent in the clear.

POP service banner. (Optional.) Use this field to enter a replacement banner for the default POP banner that is sent to a POP client when it first connects. (The default banner identifies the server version and the time of connection.)

Connection Settings

Maximum network sessions. Use this field to specify how many simultaneous POP sessions per process this server is permitted to maintain. (Default = 600.)

Drop client if idle for. Use this field to specify how long (in seconds, minutes, or hours) an idle POP connection to a client can remain open before the server drops the connection. (Default = 10 minutes.)

Process Settings

Maximum number of threads per process. Use this field to specify the maximum number of threads the POP service is permitted to have executing at a time. (Default = 1000.)

Number of processes. Use this field to specify the maximum number of processes that the POP service can employ. (Default = 1.)

Action Buttons

Save. Click this button to commit any settings you have made in the POP System form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the POP System form.

Chapter

3

Configuring SMTP Services

This chapter describes how to configure SMTP services for your server. For information on how to configure the IMAP and POP Internet-standard mailbox protocols, see Chapter 2, Configuring IMAP and POP Services.

This chapter contains the following sections:

- About SMTP
- Viewing and Configuring Domain Information
- Specifying Delivery Options
- Verifying Recipient Addresses
- Performing Host Name Resolution
- Specifying the Number of MTA Hops
- Reserving Free Disk Space
- Expanding SMTP Dialogs
- Specifying Automatic Reply Information
- Specifying Error Handling
- Specifying Routing and Addressing Information
- Controlling Access to SMTP Services
- Working With SMTP Plugins
- Managing the Message Queue
- Interface Reference: SMTP Configuration

About SMTP

Netscape Messaging Server 4.0 supports the Internet-standard Simple Mail Transfer Protocol (SMTP). SMTP is the protocol most commonly used by the Internet to define how email is transferred between computers.

User Agents (UAs), such as Netscape Communicator, use SMTP to send mail to a Message Transfer Agent (MTA). MTAs use SMTP to route messages to other MTAs within a network.

Netscape Messaging Server 4.0 listens for incoming mail on port 25 by default, the standard port for SMTP services. Incoming mail can arrive from a local mail client (UA) or from a remote MTA. For detailed concepts about how Netscape Messaging Server receives and routes messages, see Chapter 9, Message Routing.

Viewing and Configuring Domain Information

A domain identifies a site on the Internet. Messaging servers use the domain name in an email address to route messages throughout the Internet. Every email message must contain a domain name in its address.

Each Messaging Server is responsible for a particular domain or domains. These domains are considered local to the Messaging Server. If a server receives a message without a specified domain name, the server will complete the address by adding a domain name to the address. If a Messaging Server receives mail for a remote domain, it attempts to route the message to a remote MTA.

For more information about domains, the Domain Name System (DNS), and how messages are routed, see Chapter 9, Message Routing.

To view and configure information about domains, go to the SMTP System window.

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click System. The SMTP System window appears.

From this window, you can perform the following tasks:

- Specifying an Address Completion Domain
- Specifying the Domains Local to Your Server

See also SMTP System Tab in the Interface Reference section.

Specifying an Address Completion Domain

If the Messaging Server receives a message that does not contain a domain name in the recipient address, it will add the domain name to the address to complete the address. You can specify the domain name to be used for address completion. If you do not specify a domain, the domain name of the machine on which the Messaging Server resides (the default domain) is used to complete the address.

To specify an address completion domain:

1. Go to the SMTP System window.
2. In the "Address completion domain field," type the name of the DNS domain that will be used to complete a recipient address if the address does not contain a domain name.
3. Click Save.

Specifying the Domains Local to Your Server

A domain is local to your server if the Messaging Server knows the recipient addresses in the domain. The Messaging Server identifies a recipient address as local if the domain part of the address matches one of the following:

- The name of the host on which the Messaging Server resides
- The address completion domain setting
- A local domain setting

If a message is sent to a local domain, but the recipient cannot be found in the directory, the Messaging Server will bounce the message. Otherwise, the server will either deliver the message to a local mailbox or route the message to another server.

The server also checks the local domain configuration before it uses the "user ID" search method (see Specifying Alternate Search Methods). The server checks to see if the domain in the address is configured as a local domain; if the domain is local, the server will use the "user ID" search method if configured to do so.

To specify the domains local to your server:

1. Go to the SMTP System window.
2. Click the Add button beside the "Local domain" field.
3. Type the domain you want to add.
4. Click OK to add the domain to the list of local domains on the SMTP System window.

   Mail sent to an unknown recipient at any of these domains is either forwarded to another host if possible or bounced.
5. When you finished adding domain information, click Save on the SMTP System window.

   Note that changes are not saved until you click Save on the SMTP System window.

Specifying Delivery Options

You can specify the following delivery options for messages sent to your server:

- Delivering Mail to Unix Mail Folders
- Delivering Mail to a Program
- Deferring Delivery

Delivering Mail to Unix Mail Folders

For user's who have a Unix system account on the Messaging Server host machine, the Messaging Server can deliver mail to the user's local Unix mail folder. You specify the Unix mail delivery program to which the Messaging Server should deliver mail.

For users to use this feature, you must enable this feature for the user account (see Chapter 4, Managing Mail Users and Mailing Lists) and the user must turn on this option for their accounts (specified in the end user account management form).

Unix delivery is available only to users with a system account on the Messaging Server host (in addition to the Messaging Server account).

To specify a Unix mail delivery program, go to the SMTP System window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click System. The SMTP System window appears.
5. In the Local mail delivery program field, type the path of the Unix mail delivery program to which the Messaging Server should deliver mail for accounts with the Unix-delivery option enabled.

   For example: `/user/bin/mail`
6. Click Save.

See also SMTP System Tab in the Interface Reference section.

Delivering Mail to a Program

By default, messages are delivered to an account inbox. Program delivery allows messages to be delivered to external programs, such as filtering programs, file server programs, and so on.

When you or a user specifies program delivery as an account option, one or more programs are run whenever mail addressed to that account is received. The Messaging Server starts the program and delivers mail to the program.

For security reasons, Messaging Server never runs any program as "root." To enable program delivery for the root account, you must specify a safe ID for root. If a root user enables the program delivery option in the server account management forms, mail sent to root will be handled by one or more programs running under the safe ID for root.

If you do not specify a safe ID, program delivery for the root account will fail and the server will bounce messages sent to programs set up for the root account.

For more information about setting up and enabling program delivery, see Appendix B, Program Delivery.

To specify a safe ID, go to the SMTP System window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click System. The SMTP System window appears.
5. Specify information for the following fields:

   Safe user ID for running programs. In this field, type the safe Unix user ID for running programs set up for the root account.

   Safe group ID for running programs. In this field, type the safe Unix group ID for running programs set up for the root account. The safe Unix user ID should be a member of the safe group ID.
6. Click Save.

See also SMTP System Tab in the Interface Reference section.

Deferring Delivery

By default, the Messaging Server attempts to deliver messages immediately; the server queues mail only if there is a problem. You can specify that Messaging Server queue all outgoing mail and attempt delivery only when it processes the message queue. The server processes the message queue on intervals you indicate. For more information, see Managing the Message Queue.

This option is most useful for businesses that do not maintain a continuous connection to the Internet, but use dial-up connections instead. For example, the Messaging Server can dial out to a remote host and then process the mail queue for the remote host.

To specify deferred delivery, go to the SMTP Accept window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.
5. Check the "Defer delivery to remote hosts" box.
6. Click Save.

If you are specifying deferred delivery, you might also want to turn on the SMTP command, ETRN, to enable requests for deferred queue processing. With deferred queue processing, when a client (in this case, another MTA) connects to the server to send a message, it can also initiate processing of the deferred queue for the client domain. For more information, see Enabling Requests for Deferred Queue Processing (ETRN).

See also SMTP Accept Tab in the Interface Reference section.

Verifying Recipient Addresses

You can specify that the Messaging Server verify recipient addresses for messages it accepts from clients.

By enabling this option, the server can detect bad recipient names in the envelope address and return an error to the client before the client sends the body of the message. The client can fix the name before sending the message text.

Specifying this option has slight performance impact because the server must perform an LDAP lookup for each recipient while connected to the client. The benefit, however, is that bad recipients can be rejected immediately, allowing the sender to fix before sending (instead of getting a bounce message later).

To specify verification of recipient addresses, go to the SMTP Accept window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.
5. Check the "Verify each recipient's address" box.
6. Click Save.

See also SMTP Accept Tab in the Interface Reference section.

Performing Host Name Resolution

You can specify that the Messaging Server perform host name resolution for messages it accepts from clients.

Using the client's IP address, the Messaging Server will use DNS to find the associated host name. The Messaging Server will subsequently refer to client machines by host name instead of IP address. For example, host names will be used in the process table, the log file, and "Received" lines in message headers.

Note: If you handle a large volume of messages, be aware that selecting this option impacts performance adversely.

To specify that the server should perform host name resolution, go to the SMTP Accept window.

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.
5. Check the "Lookup client machine names" box.
6. Click Save.

See also SMTP Accept Tab in the Interface Reference section.

Specifying the Number of MTA Hops

Each MTA stamps all incoming messages as Received. By counting the number of Received lines in the message header, the MTA can determine how many MTAs have already handled this message. The act of routing a message from one MTA to another is called a hop or an MTA hop. Each time an MTA handles a message, the message has taken another hop.

To deliver a message might require many hops. You might want to limit the number of hops for various reasons; for example, to prevent infinite mail loops. If the number of hops exceeds the maximum you specify, the message is bounced and the server returns an error message.

To specify the maximum number of MTA hops, go to the SMTP Accept window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.
5. In the "Maximum number of MTA hops" field, specify a number.

The recommended range for this parameter is 30 or more. The default number is 30.

6. Click Save.

See also SMTP Accept Tab in the Interface Reference section.

Reserving Free Disk Space

You can specify a minimum amount of disk space that will remain unused for the message queue. If the minimum threshold is reached, the server will temporarily reject all messages until disk space is freed. The server returns an error (452) notifying the client of a temporary disk space shortage and asking the client to resend the message at a later time.

The server can also reject messages based on message size. For more information about specifying a maximum message size, see Limiting Message Size (SIZE).

To reserve free disk space, go to the SMTP Accept window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.
5. In the “Minimum free disk space” field, specify a number.
6. From the pull-down menu beside the field, specify Kbytes or Mbytes.
7. Click Save.

See also SMTP Accept Tab in the Interface Reference section.

Expanding SMTP Dialogs

Netscape Messaging Server 4.0 supports several SMTP commands for enabling extra functionality in the dialog between an SMTP client (either a UA or another server) and the Messaging Server.

To enable these commands, go to the SMTP Accept window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Accept. The SMTP Accept window appears.

From this window, you can enable SMTP commands for the following:

- Verifying User Names (VRFY)
- Verifying a Mailing List (EXPN)
- Enabling Requests for Deferred Queue Processing (ETRN)
- Limiting Message Size (SIZE)

See also SMTP Accept Tab in the Interface Reference section.

Verifying User Names (VRFY)

The VRFY command enables clients to send a request to your server to verify that mail for a specific user name resides on the server.

The server sends a response indicating whether the user is local or not, whether mail will be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name is not local, but the server can forward the message. The server response includes the mailbox name. The VRFY command is defined in RFC 821.

To enable verification of user names:

1. Go to the SMTP Accept window.
2. Check the "Allow SMTP command VRFY" box to enable the SMTP command for verifying a user name.
3. Click Save.

Caution: Because the server response might include user IDs, do not enable this option unless you are willing to reveal user IDs to clients accessing your server.

Verifying a Mailing List (EXPN)

If both the client and the server support the SMTP EXPN command, clients can make requests to your server to verify that a particular mailing list resides on the server. The EXPN command is defined in RFC 821.

To enable verification of mailing lists on your server:

1. Go to the SMTP Accept window.
2. Check the "Allow SMTP command EXPN" box to enable the SMTP command for verifying a user name.
3. Click Save.

Caution: Do not enable this option unless you are willing to acknowledge mailing lists to clients accessing your server.

Enabling Requests for Deferred Queue Processing (ETRN)

If both client (in this case another MTA) and server support the ETRN command, when the client connects to the server to send a message, it can also initiate processing of the deferred queue for the client domain. For security reasons, the server starts a new connection to the client machine before sending messages to the client. The ETRN command is defined in RFC 1985.

This feature is useful for sites that only have a dial-up connection to the Internet. By enabling this command, you can improve server performance by limiting the number of dial-up connections to your server.

To enable requests for deferred queue processing:

1. Go to the SMTP Accept window.
2. Check the "Allow SMTP command ETRN" box to enable the SMTP command for enabling requests for deferred queue processing.
3. Click Save.

Limiting Message Size (SIZE)

If both client and server support the SIZE command, clients can declare the size of a particular message to the server, and the server can accept or reject the message based on its size. Any attempts to send a message larger than the specified size will automatically fail and the server will return an error message (552) indicating that the message size exceeds the maximum allowed. The SIZE command is defined in RFC 1870.

The server can also reject a message temporarily if it is running low on disk space. For more information, see Reserving Free Disk Space.

To limit the size of messages your server accepts:

1. Go to the SMTP Accept window.
2. Check the "Allow SMTP command SIZE" box to enable the SMTP SIZE command.
3. Indicate the maximum size message the server will accept by typing a number in the field beside the checkbox and choosing MBytes or KBytes from the pull-down menu.
4. Click Save.

Specifying Automatic Reply Information

You can specify automatic reply messages for several situations. For example, you can specify a default vacation reply message for users who do not write a personalized message or you can specify a default reply for messages sent to a particular address.

To specify automatic reply information, go to the SMTP Autoreply window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Autoreply. The SMTP Autoreply window appears.
5. From the pull-down menus for each field, choose the language of your choice.
6. Type the default messages for each of the reply fields:

   Default vacation-mode reply message. Type an automatic reply for users who do not write a personalized vacation message.

   Anyone who sends messages to a user's account while the vacation setting is activated will receive one notice about the user's absence. Any subsequent messages that person sends are ignored.

   In most cases, you should not replace a user's current delivery with the vacation setting when they set up the AutoReply handler for that user's account. If you do this, the user will return from vacation only to find that all of his or her email has been thrown away. Rather, you should use the vacation setting in addition to the normal delivery method, so mail is held for the user to retrieve upon his or her return. (Users are prevented from making this mistake because the Messaging Server doesn't accept account management forms with a delivery of "Vacation" only.)

   Default echo-mode reply message. Type an automatic reply for the server's echo feature. A common use of the echo feature is to return mail addressed to people who have moved on and left no forwarding address.

The echo feature generates a message to anyone who sends a message to the account. In addition, it returns the mail (as a MIME attachment) that was sent to the account, so that the sender gets back the original message as well as the message that you entered.

The echo feature, like the vacation feature, is intended to inform people about the status of the account they have contacted.

Default reply-mode reply message. Type an automatic reply for the server's default reply mode.

The default reply feature is useful for special accounts that are created to disseminate information of one kind or another. You can create a place where people can get files, analogous to a File Transfer Protocol (FTP) site on the Internet.

7. Click Save

See also SMTP Autoreply Tab in the Interface Reference section.

Specifying Error Handling

There are various situations in which an MTA cannot deliver or route a message. For example, the most common are when an address refers to an unknown local account, when the maximum number of MTA hops is exceeded, or when disk quota is exceeded.

To specify error handling instructions, go to the SMTP Error window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Error. The SMTP Error window appears.
5. For each error situation, choose one of the following error handling methods:
   - Return message to sender
   - Notify the postmaster via email

- Log the error in the log file

6. Click Save.

See also SMTP Error Tab in the Interface Reference section.

Specifying Routing and Addressing Information

For detailed conceptual information about routing and addressing, including information about envelope rewrite methods, alternate search methods, and the SMTP routing table, see Chapter 9, Message Routing.

To specify routing and addressing information, go to the Address window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click Address. The SMTP Address window appears.

From this window, you can perform the following tasks:

- Specifying Envelope Rewrite Methods
- Specifying From Address Rewrite Style
- Specifying Alternate Search Methods
- Editing SMTP Routing Table Entries

Note: You should shut down your server before specifying configuration changes on this form.

See also SMTP Address Tab in the Interface Reference section.

Specifying Envelope Rewrite Methods

You can specify whether and how the server rewrites the envelope recipient address before routing a message to a remote MTA. To specify envelope rewrite methods:

1. Go the SMTP Address window.

2. Check one or more of the following boxes:

   Use the mailRoutingAddress attribute. This method is most useful for LDAP entries that represent mail accounts on non-Netscape mail servers or gateway systems.

   Note that you must also modify the user's LDAP entry (by using `ldapmodify`) to include the `mailRoutingAddress` attribute.

   Combine the uid with the mailHost attribute. With this method, the server combines the `uid` attribute and the `mailHost` attribute found in the LDAP directory for rewriting the envelope address.

   For example, mail arrives on one server for `Joe_Smith@airius.com`. The server determines that this mail belongs to `jsmith` whose mail account is on `judge.airius.com`. The server rewrites the envelope address to `jsmith@judge.airius.com` then relays the message to `judge.airius.com`.

   This method is most likely to work properly if the "uid" search method is employed on the next server.

   Some sites prefer that only explicit addresses (that is, those addressed specified by the `mail` and `mailAlternateAddress` attributes) are valid email addresses for users. You should not use this method if the local policy does not consider `uid` a valid email address.

   Combine the local part of the address with the mailHost attribute. With this method, the server combines the local part of the original address with the `mailHost` attribute value to create the new address.

   For example, `Customer_Service@airius.com` becomes `Customer_Service@judge.airius.com`. This method is useful to support entities, such as mail groups, that do not have a uid.

This method is not used if the "custom domain" search method is used to resolve the address. You should not use this rewrite method if changing the domain part to a specific host creates ambiguity about the message recipient.

3. Click Save.

The default method is to use the original address unmodified.

Specifying From Address Rewrite Style

Rewriting the "From:" address increases the odds that replies to outgoing messages are processed correctly. For example, often the address that a mail client inserts in the "From:" line isn't the best choice. To specify how the server should rewrite the "From" address:

1. Go to the SMTP Address window.
2. From the "From address rewrite style" pull-down menu, choose one of the following rewrite styles:

   "john doe"<jdoe@company.com>. Choose this option to rewrite the address in the style indicated.

   jdoe@company.com (John Doe). Choose this option to rewrite the address in the style indicated.

   jdoe@company.com. Choose this option if you want the server to try to complete an incomplete address.

   never rewrite addresses. Choose this option if you do not want the server to rewrite any part of the from address.

   You might want to choose this option, for example, if you have a plug-in program that performs address rewrites. Or, for another example, in a multilingual environment where you trust the sender to use the appropriate alphabet and do not want to modify the address.

3. Click Save.

Specifying Alternate Search Methods

You can expand the list of possible recipient matches by specifying one or more of the following search methods. If all search methods are specified, the server tries each method in the order listed until a match is found. The default setting is search on user ID only.

To specify alternate search methods:

1. Go to the SMTP Address window.

2. Check one ore more of the following boxes:

   Search for custom domain. Check this box if you want the server to use the "custom domain" search method.

   Assume Joe has two addresses with his ISP: `joe@isp.com` and a custom domain address, `joecorp.com`. To enable Joe to receive mail addressed to *`anything`*`@joecorp.com`, you must add a `MailAlternateAddress` value for Joe as follows: `@joecorp.com`. You must also add the MX records in DNS as necessary to indicate the desired messaging server for the custom domain. For more information about DNS and MX records, see The Domain Name System (DNS) in Chapter 9.

   Search using truncated domain. Check this box if you want the server to use the "truncated domain" search method.

   In a network environment, you might want the option of ignoring the host name when searching for an address. For example, assume the following: The value for `MessageHostName` is `foo.airius.com`; Joe's email address is `joe@airius.com`. With this feature enabled, the server can ignore the host name `foo` when searching in the directory for the correct address. Consequently, Joe can receive messages addressed to both `joe@foo.airius.com` and `joe@airius.com`.

   You should use this feature only if user accounts are not specific to a particular host. For example, if `user@host1.domain.com`, `user@host2.domain.com`, and `user@domain.com` are considered different accounts, do not enable this feature.

   Search by user ID. Check this box if you want the server to use the "user ID" search method.

The server can search on the user ID only if 1) the domain in the address matches one of the host values specified for the `MessageHostName` parameter or 2) the domain is configured as a local mail domain.

With this feature enabled, each user's `uid` attribute in LDAP is a valid email address for that user in an address such as `uid@LocalMailDomain` or `uid@MessageHostName`.

Do not use this feature if you do not want the user's `uid` to be treated as a valid email address.

3. Click Save.

Note: Specifying alternate search methods has a slight impact on performance.

Editing SMTP Routing Table Entries

If the Messaging Server assumes another mail server is responsible for this recipient, the Messaging Server checks its mail routing table to see if mail for the recipient's domain should be routed to a specific mail server host.

Entries in the mail routing table are processed in order. You should keep this in mind when creating entries. For example, if you have an entry that sends all non-local mail to a firewall mail server, you want this entry to be the last entry in the routing table.

To edit SMTP routing table entries:

1. Go to the SMTP Address window.
2. Click the Add button by the SMTP routing table field.
3. Type a routing table entry.
4. Click OK to return to the SMTP Address window.
5. Click Save.

Example Routes

The following example routes all internal mail through a hub server:

```
*.airius.com:hub.airius.com
```

The next example forces the use of IP addresses for frequently called servers (bypassing DNS):

```
hub.airius.com:[123.345.456.7]
```

The next example shows the use of a firewall server for all outside mail:

```
*airius.com:*
*:firewall.airius.com
```

Controlling Access to SMTP Services

Netscape Messaging Server provides several features that enable you to control access to your SMTP services. These features include:

- Specifying authenticated SMTP
- Specifying access control filters
- Filtering unsolicited bulk email (UBE)

Netscape Messaging Server also supports the Secure Sockets Layer (SSL) protocol for transferring private data over TCP/IP networks. For details about determining the access control and security requirements for your server, see Chapter 6, Security and Access Control.

Specifying Authenticated SMTP

Authenticated SMTP provides for greater security in sending messages using the SMTP protocol. To use authenticated SMTP, you do not need to deploy a certificate-based infrastructure. However, authenticated SMTP does not provide the same level of security features as a certificate-based infrastructure.

With authenticated SMTP, the client (either a user agent or another server that supports authenticated SMTP) can indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. For example, when supported by the user's mail client, authenticated SMTP can require users to enter a password before they are allowed to send messages.

For more information about authenticated SMTP, and when and how to use it in your security and access scheme, see Chapter 6, Security and Access Control.

To specify authenticated SMTP, go to the SMTP System window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services folder.
3. Click SMTP. The SMTP configuration tabs appear in the right pane.
4. Click System. The SMTP System window appears.
5. Check the "Allow password login" box.
6. Specify a minimum cipher length for password encryption.

   A cipher is the algorithm used to encrypt and decrypt data in the encryption process. A cipher operates on data by applying a key--a long number--to the data. Generally, a longer key represents a more secure encryption process.

   Caution: If you specify 0, the server does not encrypt passwords. Do not specify 0 if you are concerned about sending passwords in clear text. Choose 40 or 128 to ensure that passwords are sent over secure channels.
7. Click Save.

See also SMTP System Tab in the Interface Reference section.

Specifying Access Control Filters

You can define access control filters to exclude spammers and DNS spongers from your system and improve the general security of your network.

For detailed information about TCP client access control features including complete filter syntax, see the chapter entitled Chapter 6, Security and Access Control. For details about how to define access control filters for your SMTP services, see Creating Access Filters with Netscape Console in Chapter 6.

Filtering Unsolicited Bulk Email

Unsolicited Bulk Email (UBE) is email sent to large number of recipients without their knowledge or consent, often advertising commercial products or services. It is the electronic equivalent of paper "junk mail."

Netscape Messaging Server provides an SMTP UBE plugin you can use to design and implement filters that block unsolicited bulk email from reaching your servers.

For details about the UBE plugin and how to use it to filter unwanted mail, see Chapter 8, Filtering Unsolicited Bulk Email.

Working With SMTP Plugins

Netscape Messaging Server 4.0 provides an application programming interface (API) that allows third parties to create server plugins that can add site-specific functionality to the Messaging Server.

For details on working with SMTP plugins, see Chapter 7, Working With SMTP Plug-Ins.

Managing the Message Queue

By default, the Messaging Server attempts to deliver messages immediately; the server queues mail only if there is a problem, or if you have explicitly specified deferred delivery to other servers. (For information about specifying deferred delivery, see Deferring Delivery.)

This section discusses two types of queues: logical queue and physical queue.

Logical Queue. Logical queue refers to the active queue (the messages currently being processed) and one or more deferred queues (messages that are queued for future delivery).

Deferred messages are grouped by domain. If the server cannot deliver mail to a domain, it automatically creates a logical queue based on the domain part of the message address and the physical queue containing the message.

You can manage logical queues as described in the following sections:

- Specifying Actions on Logical Queues
- Enabling Requests for Deferred Queue Processing (ETRN)

Physical Queue. A physical queue refers to where and how messages are stored on disk. You can specify alternate path names for physical queue directories, as described in Specifying Alternate Paths for Queue Storage.

About the Queue Directories

Logical queues are stored across three physical queue directories: `control`, `deferred`, `messages`.

The control Directory

The `control` directory contains the information necessary to process messages in the active queue--the queue that the Messaging Server is currently processing.

When the server accepts a message, it logs an entry in the `control` directory. When the server is finished processing the message (the message has been delivered to the user's inbox, the message has been deferred, or the message has been relayed), the server logs another entry in the `control` directory.

The `control` directory entries contain pointers to files in the `messages` directory.

The deferred Directory

The `deferred` directory contains the control information for messages that have been deferred. This directory contains one file to record the information about deferred messages.

The `deferred` directory entries contain pointers to the files in the `messages` directory.

The messages Directory

The `messages` directory contains the text (header and body) of all messages in the active and deferred queues. This directory contains one file per message.

Specifying Actions on Logical Queues

You can specify whether to return messages to the sender, move messages to the active queue, or delete messages from the queue.

To specify actions on a logical message queue, go to the Queued Messages window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services Folder.
3. Click SMTP.
4. Click Message Queue. The Message Queue configuration tabs appear in the right pane.
5. Click Queued Messages. The Queued Messages window appears.
6. Select a queue from the list.
7. Click the Select Action button.
8. Select an action from the pop-up window and click OK.
9. Click Save.

See also Queued Messages Tab in the Interface Reference section.

You can enable requests for processing of deferred queues to limit the number of dial-up connections to your server. With deferred queue processing, when a client (in this case another MTA) connects to the server to send a message, it can also initiate processing of the deferred queue for the client domain. For more information, see Enabling Requests for Deferred Queue Processing (ETRN).

You can also perform actions on the queue from the command line interface. For more information about the command line utilities for managing the queue, see `mailq` and `processq` in Appendix A.

Specifying Alternate Paths for Queue Storage

You can specify alternate MTA queue paths for the physical queue directories: `control`, `messages`, and `deferred`..

By specifying alternate MTA queue paths, you can distribute the load associated with delivering a message because the server can perform concurrent I/O operations. You can also reduce the overhead associated with large numbers of files accumulating in a single message queue.

To specify an alternate path for queue storage, go to the Message Queue Configuration window:

1. In the Messaging Server Console, select the Configuration tab.
2. Open the Services Folder.
3. Click SMTP.
4. Click Message Queue. The Message Queue configuration tabs appear in the right pane.
5. Click Configuration. The Message Queue Configuration window appears.
6. Click the Add button beside the Queue path field.
7. Type a queue path and click OK.
8. Click Save.

See also Message Queue Configuration Tab in the Interface Reference section.

Interface Reference: SMTP Configuration

This section describes the Messaging Server interface elements that allow you to configure and execute the server's SMTP services. You access these elements through Netscape Console; see *Managing Servers With Netscape Console* for information on using Netscape Console to manage the Messaging Server and other Netscape servers.

SMTP System Tab

You use the form accessed through the SMTP System tab to specify information about domains, authenticated SMTP, and delivery options. For more information, see also:

- Viewing and Configuring Domain Information
- Specifying Authenticated SMTP
- Specifying Delivery Options

Domains

Address completion domain. In this field, type the name of the DNS domain that will be used to complete a recipient address if the address does not contain a domain name.

Local domain. This field displays the mail domains handled by this MTA. You can add a domain or edit the contents of this field by clicking one of the following three buttons. Mail sent to an unknown recipient at any of these domains is either forwarded to another host if possible or bounced.

Add. Click this button to bring up a window (see Add Domain Window) that allows you to add a new domain to the Local Domain field.

Edit. Click this button to bring up a window that allows you to edit the domain that is currently highlighted in the Local Domain field.

Delete. Click this button to delete the domain that is currently highlighted in the Local Domain field.

Authenticated SMTP

Allow password login. Check this box to allow authenticated SMTP.

Minimum cipher length for password encryption. Choose the minimum cipher length for password encryption from the pulldown menu: 0, 40, or 128.

Unix Delivery

Local mail delivery program. In this field, type the path of the Unix mail delivery program to which the Messaging Server should deliver mail for accounts with the Unix-delivery option enabled.

For more information about Unix delivery, see Delivering Mail to Unix Mail Folders earlier in this chapter.

Program Delivery

Safe user ID for running programs. In this field, type the safe Unix user ID for running programs set up for the root account.

Safe group ID for running programs. In this field, type the safe Unix group ID for running programs set up for the root account. The safe Unix user ID should be a member of the safe group ID.

For more information about program delivery, see Delivering Mail to a Program earlier in this chapter.

Action Buttons

Save. Click this button to save settings you have made in the SMTP System window.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the SMTP System window.

Add Domain Window

You use the Add Domain window to add a domain to the list of domains handled by this MTA. For more information, see also:

- Viewing and Configuring Domain Information
- Specifying the Domains Local to Your Server
- The Domain Name System (DNS)

Domain handled by this server exclusively. Type the domain name you want to add.

OK. Click this button to add the domain to the list of local domains on the SMTP System window.

Note that changes are not saved until you click Save on the SMTP System window.

Cancel. Click this button to cancel edits you've made to the Add Domain window.

Help. Click this button to get online help (this document) describing the Add Domain window.

SMTP Accept Tab

You use the form accessed through the SMTP Accept tab to specify information about message delivery, address verification, host name resolution, the maximum number of MTA hops allowed, minimum free disk space, and whether the server allows various SMTP commands. For more information, see also:

- Deferring Delivery
- Verifying Recipient Addresses
- Performing Host Name Resolution
- Specifying the Number of MTA Hops
- Reserving Free Disk Space
- Expanding SMTP Dialogs

Defer delivery to remote hosts. Check this box to defer delivery to remote MTAs. If you check this option, the Messaging Server queues all outgoing mail and attempts delivery only when it processes the message queue.

Verify each recipient's address. Check this box if you want the Messaging Server to verify each address listed as a recipient. The Messaging Server returns an error for local addresses that are not found in the Directory Server.

Lookup client machine names. Check this box if you want the Messaging Server to perform host name resolution for all connecting client machines.

Maximum number of MTA hops. In this field, type the maximum number of times a message can be routed from one MTA to another. The recommended range for this parameter is 30 or more. The default number is 30.

Minimum free disk space. In this field, type the minimum amount of disk space that should remain free. You can specify MBytes or KBytes from the pull-down menu. If disk space gets too low according to the value you specify, the server will reject messages temporarily.

Allow SMTP command 'VRFY'. Check this box to enable the SMTP command for verifying a user name.

> **Caution:** Because the server response might include user IDs, do not enable this option unless you are willing to reveal user IDs to clients accessing your server.

Allow SMTP command 'EXPN'. Check this box to enable the SMTP command for verifying a mailing list. If both client and server support the EXPN command, clients can make requests to your server to verify that a particular mailing list resides on the server.

> **Caution:** Do not enable this option unless you are willing to acknowledge mailing lists to clients accessing your server.

Allow SMTP command 'ETRN'. Check this box to enable the SMTP command for enabling requests for deferred queue processing.

Allow SMTP command 'SIZE'. Check this box if you want to enable client/server dialog about message size. Indicate the maximum size the message the server will accept by typing a number in the field beside the checkbox and choosing MBytes or KBytes from the pull-down menu.

Action Buttons

Save. Click this button to save settings you have made in the SMTP Accept window.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the SMTP Accept window.

SMTP Autoreply Tab

You use the form accessed through the SMTP Autoreply tab to specify automatic reply messages for various situations. For more information, see also Specifying Automatic Reply Information.

Default vacation-mode reply message. In this field, type the vacation message that will be used if users do not write a personalized message. The MTA automatically sends this reply message for a user account whose vacation setting is activated.

Default echo-mode reply message. In this field, type a generic message for users sending messages to this address. A common use of the echo feature is to return mail addressed to people who have moved on and left no forwarding address.

Default reply-mode reply message. In this field, type a message that can be used to advise the sender to contact the server administrator.

Save. Click this button to save settings you have made in the SMTP Autoreply window.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the SMTP Autoreply window.

SMTP Error Tab

You use the form accessed through the SMTP Error tab to specify how the server should handle error messages. For more information, see also Specifying Error Handling.

Return message to sender. Check this box to return an error message to the sender of the message.

Notify the postmaster via email. Check this box to notify the postmaster of the error via email.

Log the error in the log file. Check this box to log the error in the log file.

Save. Click this button to save settings you have made in the SMTP Error window.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the SMTP Error window.

SMTP Address Tab

You use the form accessed through the SMTP Address tab to specify options for envelope rewrite methods, "From" address rewrite style, alternate search methods, and SMTP routing table entries. For more information, see also:

- Specifying Routing and Addressing Information
- Specifying Envelope Rewrite Methods
- Specifying From Address Rewrite Style
- Specifying Alternate Search Methods
- Editing SMTP Routing Table Entries

Note: You should shut down your server before specifying configuration changes on this form.

Envelope Rewrite Methods

Use the mailRoutingAddress attribute. Check this box if you want the server to use a specific mail routing address for rewriting the message envelope. This method is most useful for LDAP entries that represent mail accounts on non-Netscape mail servers or gateway systems.

You must also modify the user's LDAP entry (for example, by using `ldapmodify`) to include the `mailRoutingAddress` attribute.

Combine the uid with the mailHost attribute. Check this box if you want the server to combine the `uid` attribute and the `mailHost` attribute found in the LDAP directory for rewriting the envelope address.

Combine the local part of the address with the mailHost attribute. Check this box if you want the server to combine the local part of the original address with the `mailHost` attribute value to create the new address.

From Address Rewrite Style

"john doe"<jdoe@company.com>. Choose this option to rewrite the address in the style indicated.

jdoe@company.com (John Doe). Choose this option to rewrite the address in the style indicated.

jdoe@company.com. Choose this option if you want the server to try to complete an incomplete address.

never rewrite addresses. Choose this option if you do not want the server to rewrite any part of the from address.

Alternate Search Methods

Search for custom domain. Check this box if you want the server to use the "custom domain" search method.

Search using truncated domain. Check this box if you want the server to use the "truncated domain" search method.

Search by user ID. Check this box if you want the server to use the "user ID" search method.

SMTP Routing Table

SMTP Routing table. This field displays SMTP routing table entries. You can edit the contents of this field by highlighting a line in this field and then clicking one of the following three buttons.

Add. Click this button to bring up a window (see Add Routing Table Entry Window) that allows you to add a new routing table entry.

Edit. Click this button to bring up a window that allows you to edit the routing table entry that is currently highlighted in the Routing table field.

Delete. Click this button to delete the routing table entry that is currently highlighted in the Routing table field.

Action Buttons

Save. Click this button to save settings you have made in the SMTP Address window.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the SMTP Address window.

Add Routing Table Entry Window

You use the Add Routing Table Entry window to add or edit routing table entries.

Routing table entry. In this field, type the routing table entry you want to add.

Entries in the mail routing table are processed in order. You should keep this in mind when creating entries. For example, if you have a route entry that sends all non-local mail to a firewall mail server, you would want this entry to be the last entry in the routing table.

OK. Click this button to add the entry to the list of entries on the SMTP Routing Table field on the SMTP Address window.

Note that changes are not saved until you click Save on the SMTP Address window.

Cancel. Click this button to cancel edits you've made to the Add Routing Table Entry window.

Help. Click this button to get online help (this document) describing SMTP routing table entries.

SMTP Access Tab

You use the form accessed through the SMTP Access tab to control access to the SMTP service. For more information on this form, see SMTP Access Tab in Chapter 6.

Queued Messages Tab

You use the form accessed by the SMTP Queued Messages tab to view information about logical message queues and specify actions on the queues. For more information, see also Managing the Message Queue.

Queue List. The queue list shows the active queue and the deferred queues that currently exist on the server. For each queue, the queue list shows the name of the queue, the number of messages in the queue, and the actions specified for the queue. The active queue is the queue currently being processed by Messaging Server. There can be only one active queue.

Select Action. Click this button to bring up a window that allows you to specify an action on a particular deferred queue (see Queued Messages Action Window). You cannot select an action for the active queue.

Save. Click this button to start the actions specified in the Queued Messages Action window on the queues.

Reset. Click this button to reset the window to the current server settings.

Help. Click this button to get online help (this document) describing the Queued Messages window.

Queued Messages Action Window

You use the Queued Messages Action window to indicate an action to be performed on the selected deferred queue. You cannot specify an action on the active queue. For more information, see also Specifying Actions on Logical Queues.

Bounce. Click this option if you want return all messages in the queue to the sender.

Delete. Click this option if you want to delete messages in the queue.

Requeue. Click this option if you want to move messages in the queue to the active queue.

OK. Click this button to add the action to the Queued Messages window.

Note that the actions are not carried out until you click Save on the Queued Messages window.

Cancel. Click this button to cancel selections you've made to the Queued Messages Action window.

Help. Click this button to get online help (this document) describing the message queue actions.

Message Queue Configuration Tab

You use the from accessed by the Message Queue Configuration tab to specify alternate physical locations for queues and to specify processing information for the deferred logical queues. For more information, see also:

- Managing the Message Queue
- Specifying Alternate Paths for Queue Storage

Alternate MTA Queues

Queue path. This field displays alternate MTA queue paths.

Add. Click this button to bring up a window (see Add MTA Queue Window) that allows you to add a new queue path to the Queue path field.

Edit. Click this button to bring up a window that allows you to edit the queue path that is currently highlighted in the Queue path field.

Delete. Click this button to delete the queue path that is currently highlighted in the Queue path field.

Processing Information

Message queue process interval. In this field, type a number to indicate how often Messaging Server processes the deferred message queues. From the pull-down menu, you can specify seconds, minutes, or hours.

Maximum message queue time. In this field, type a number to indicate the maximum time messages can remain in the deferred queue. After this time, messages are deleted from the queue. From the pull-down menu, you can specify hours or days.

Add MTA Queue Window

You use the Add MTA Queue window to add an alternate message queue path. For more information, see also Specifying Alternate Paths for Queue Storage.

Path name of the MTA queue. Type the path name of the alternate queue.

OK. Click this button to add the path name to the list of alternative queues on the SMTP System window.

Note that changes are not saved until you click Save on the Message Queue Configuration window.

Cancel. Click this button to cancel edits you've made to the Add MTA Queue window.

Help. Click this button to get online help (this document) describing the Add MTA Queue window.

Chapter

4

Managing Mail Users and Mailing Lists

This chapter explains how mail accounts and mailing lists are implemented in Messaging Server 4.0, and it describes how to use the Netscape Console interface to create and manage your users' mail accounts and mailing lists.

This chapter contains the following sections:

- About Users and Groups for Messaging
- Managing Mail Users
- Managing Mailing Lists
- Interface Reference: Managing Mail Users

About Users and Groups for Messaging

Messaging Server 4.0 requires close integration with an LDAP directory service such as Netscape Directory Server. One reflection of this close integration is the manner in which mail accounts and mailing lists are implemented.

Users and Mail Accounts

An LDAP user directory can contain a wide range of information about an organization's employees, members, clients, or other types of individuals that on one way or another "belong" to the organization. These individuals

constitute the *users* of the organization. In the LDAP directory, the information about users is structured for efficient searching, with each user entry identified by a set of attributes. Directory attributes associated with a user can include name and other identification, division membership, job classification, physical location, name of manager and direct reports, access permission to various parts of the organization, preferences of various kinds, and so on.

In an organization with electronic messaging services, many if not all users hold mail accounts. For Messaging Server 4.0, mail-account information is not stored locally on the server; it is part of the LDAP user directory. The information for each mail account is stored as a particular set of attributes attached to a user's entry in the directory. To retrieve or modify information for a specific user's mail account, an administrator uses the Messaging Server interface to access that user's mail attributes in the directory.

Groups and Mailing Lists

An LDAP user directory also can contain entries that represent collections of users. These directory *groups* can consist of a specific set of users or they can be rule-based, with membership defined by job classification or any other user attributes.

Groups can exist for a wide variety of purposes, and they have their own sets of attributes in the user directory. Groups may be used for information sharing in departments or on projects, for providing selective access to sensitive data, for discussion on shared interests, for disseminating company or division policy, and so on.

Messaging Server 4.0 provides support for mailing lists, which can be thought of as group addresses (similar to `sendmail` aliases) with additional associated information (such as a set of access permissions for posting to the list). As with mail-account information, Messaging Server stores mailing-list information in the LDAP user directory rather than locally. The information is stored as a set of attributes belonging to a particular group. To retrieve or modify information for a specific mailing list, an administrator uses the Netscape Console interface to access the appropriate group's attributes in the user directory.

A mailing list can exist as its own group in the directory, or mailing-list capability can be added to any existing directory group.

Mail-Administration Features

You use the mail-administration portion of the Netscape Console interface to configure and administer the mail accounts and mailing lists hosted by your Messaging Server. These are the general tasks you can perform:

For any user in your user directory, you can

- access the user as a mail account
- specify mail addressing information for the account
- define the delivery method(s) and attributes for the account
- specify forwarding addresses and attributes for the account
- specify auto-reply procedures for the account

For any group in your user directory, you can

- access the group as a mailing list
- specify mail addressing information for the mailing list
- specify (mailing-list-only) members for the mailing list
- define restrictions for posting messages to the mailing list
- define and enable message-rejection actions for the mailing list

Subsequent sections in this chapter give detailed discussions of these administrative tasks. Before you can perform them, however, you must first enable the mail-administration interface, as described in the next section.

> **Note:** For entry or manipulation of large numbers of mail accounts, it may be more efficient to use bulk methods than to use the Netscape Console interface described here. For more information, see the discussion on migration tools in Appendix A, Command-line Utilities, and Appendix C, sendmail Migration and Compatibility.

Managing Mail Users

Accessing Mail Users

This section describes how to get to the mail administration interface for your users. Because Messaging Server mail accounts are stored as attributes of user entries in an your enterprise's central LDAP user directory, managing mail accounts means accessing and modifying user entries in that directory.

Creating a New User

To create a new mail account, you create a new user in the directory. You must also install a mail account for that user; if you do not install the mail account, the mail-administration portion of Netscape Console is not available. (The full process of creating a user and specifying other kinds of user information is described in more detail in *Managing Servers with Netscape Console*).

To create a new mail user:

1. In the Netscape Console main window, click the Users and Groups tab. The Users and Groups window opens.
2. Select New User and click Create. After you select an organizational unit for the user, the Create User window opens (see Figure 4.1).
3. Enter at least the required information to create the user entry, as noted in the Users and Groups chapter of *Managing Servers with Netscape Console*.
4. Before closing the Create User window, click the Account tab. A list of installable products for the new user's account appears in the right pane (see Figure 4.2).
5. Click the Mail Account Install box. The Mail tab becomes visible in the Create User window.
6. Click on the Mail tab in the Create User window, then click the appropriate tab in the right pane to go to the desired form (see Figure 4.3).

   (These are the forms described in this chapter.)

7. Enter your changes, then click OK at the bottom of the Create User window. This submits your entries and dismisses the Create User window.

   Note. Clicking OK at the bottom of any mail administration form submits all of the current mail configuration information entered into all of the mail administration forms. Make sure you complete all setup procedures in the relevant forms before clicking OK.

Figure 4.1 Create User window (without Mail tab)

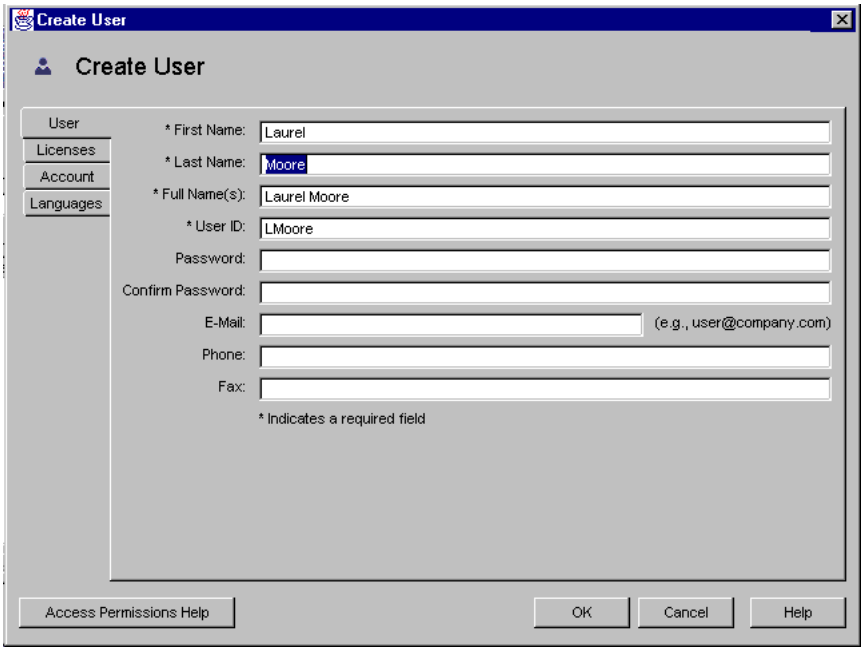


Figure 4.2 Create User window with Install Mail Account option

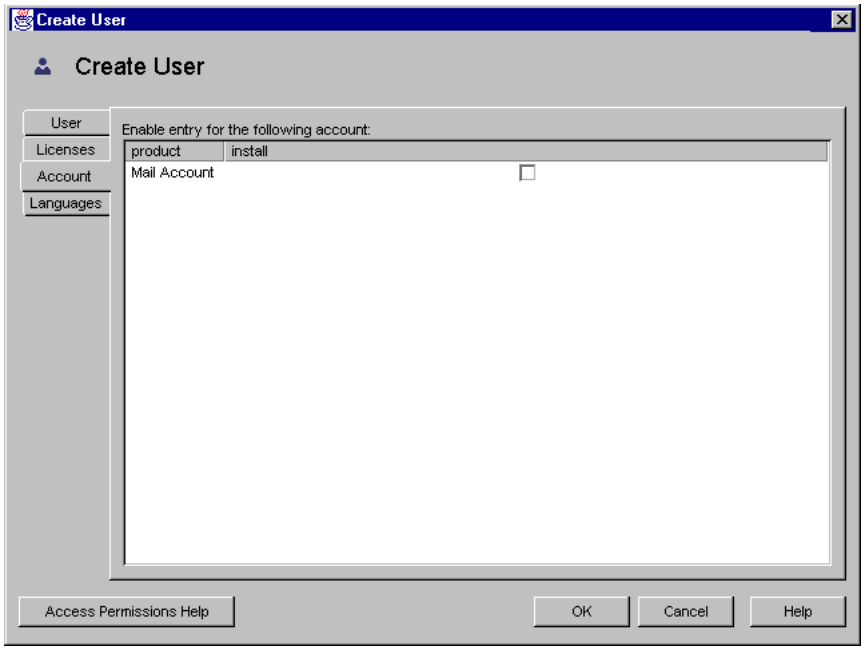
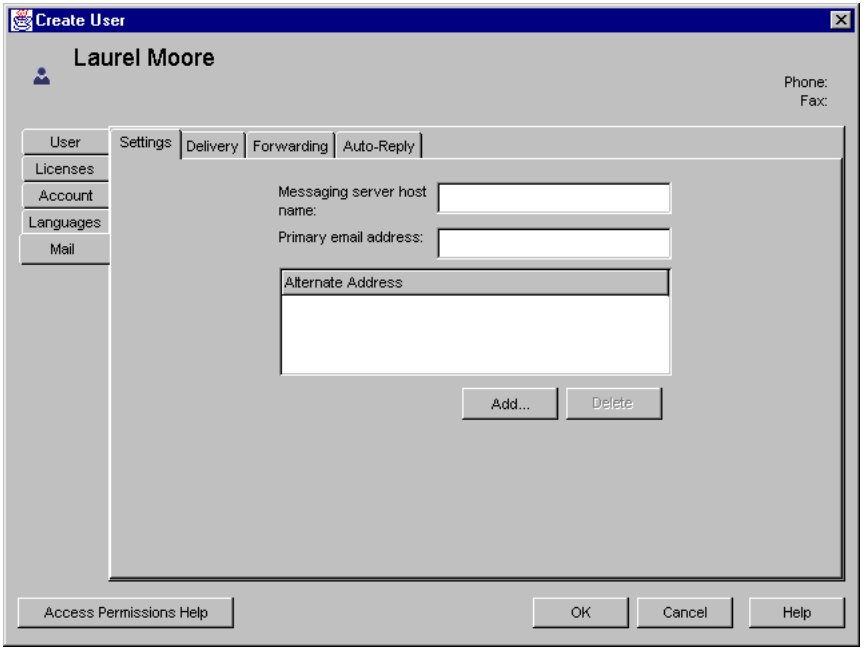


Figure 4.3 Create User window with mail account installed (Mail tab selected)



Accessing an Existing User

To modify an existing mail account or to add a mail capabilities to an existing user, you access the appropriate user in the user directory and then add or modify that user's mail-account attributes.

To access mail information for an existing user:

1. In the Netscape Console main window, click the Users and Groups tab.
2. In the Users and Groups main window, Click Search or Advanced Search.
3. Enter your search criteria (such as the user's last name) in the Search window, and perform the search of the user directory.
4. Back in the Users and Groups main window, select a user from the search results and click Edit. The Edit Entry window opens.
5. If the Mail tab is not visible in the Edit Entry window, do this:

- Click the Account tab. A list of installable accounts appears in the right pane (see Figure 4.2).
- Check the Mail Account Install box. The Mail tab now becomes visible in the Edit Entry window.

6. Click the Mail tab in the Edit Entry window, then click the appropriate tab in the right pane to go to the desired form.

   (These are the forms described in this chapter; they are identical to those you access through Create User window.)

7. Enter your changes, then click OK at the bottom of the Edit Entry window. This submits your modifications and dismisses the Edit Entry window.

Specifying User Email Addresses

Before mail can be delivered successfully to a user, you must specify the mail addressing information for that user. This consists of the Messaging Server host name, the user's primary address, and any alternate addresses. The host name and primary address information is mandatory; alternate address information is optional.

To specify a user's mail addressing information:

1. In Netscape Console, access the Create User or Edit Entry window, as described in Accessing Mail Users.
2. Click the Mail tab.
3. Click the Settings tab, if it is not already frontmost. The Settings form is displayed.
4. (Required) Enter the Messaging Server hostname.

   This is the machine hosting the Messaging Server that will process this user's mail. This must be the fully-qualified domain name (FQDN) known to the Messaging Server on that machine.

5. (Required) Enter the user's primary email address.

This is the publicized address to which this user's mail is to be sent. There can be only one primary address for a user, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

If you want to implement hostname hiding (the host name in the user's address is not to be shown in the outgoing mail header) do not specify the host name in the Primary email address field.

6. (Optional) If you want to add an address to the Alternate Address list, click Add to go to the Add Alternate Address window.

   An alternate address is essentially an alias for the user's primary address. You can use this feature, for example, to ensure proper delivery of frequently misspelled addresses (e.g., "Smith" as an alias for "Smythe"), or for host name hiding in outgoing mail headers. You can specify any number of alternate addresses for a particular user, as long as each address is unique. Messages arriving for any of these aliases are directed to the primary address.

   Enter the user's alternate address in the address field (you cannot enter more than one address each time you open this window).

   Click OK to add the address and dismiss the Add Alternate Address window.

   (See Add Alternate Address Window for a complete description of the contents of this window.)

7. Click OK in the Settings form if this action completes all changes that you wish to make to this user's mail information. Otherwise, click other tabs to continue making entries in other forms.

See Mail Settings Tab for a complete description of the contents of this form.

Configuring Delivery Options

The Messaging Server supports three principal mail-delivery options that you can enable and configure, in any combination, for each user. You can provide regular POP/IMAP delivery, program delivery, and Unix delivery (for clients of a Unix Messaging Server host).

Messaging Server also provides an end-user HTML interface through which users can themselves enable and configure these options. The Netscape Console (administrator) interface and the HTML (user) interface both manipulate the same directory attributes; when opened, each shows the current settings, whether they were set by the administrator or by the user.

To configure delivery options for a user:

1. In Netscape Console, access the Create User or Edit Entry window, as described in Accessing Mail Users.
2. Click the Mail tab.
3. Click the Delivery tab. The Delivery Options form is displayed.
4. Select the delivery method or methods you want to enable for this user:
   - To specify POP/IMAP delivery, follow the instructions in Specifying POP/IMAP Delivery (next).
   - To specify program delivery, follow the instructions in Specifying Program Delivery.
   - To specify Unix delivery, follow the instructions in Specifying Unix Delivery.
5. Click OK in the Delivery Options form if this action completes all changes that you wish to make to this user's mail information. Otherwise, click other tabs to continue making entries in other forms.

See Delivery Options Tab for a complete description of the contents of this form.

Specifying POP/IMAP Delivery

Specifying this option enables mail delivery to the user's regular POP3 or IMAP4 mailboxes. To enable POP/IMAP delivery for this user:

1. Access the Delivery Options form.
2. Check the POP/IMAP box, and click the Properties button to open the POP/IMAP Delivery window.

3. Enter the nickname of message-store partition to which the user's messages are to be delivered and stored for processing. If you leave this field blank, the current primary partition is used. See Chapter 5, Managing the Message Store, for more information.

4. Enter the storage limit, or disk quota, to be allotted to the user. The quota can be either unlimited (no maximum storage limit), or you can specify a limit (KB or MB). Unlimited is the default.

5. Note the contents of the Access domain field. Access domains are domains from which this user is permitted to retrieve mail. If no access domains are specified in the Access domain field, this user can retrieve mail from any domain. Entries in this field can be either domain names or IP addresses.

   If you want to specify access domains, click Add next to the Access Domains field. The Add Access Domains window opens.

6. Enter a domain name in the Access domain name field.

   You must enter only a single domain name each time you access the Add Access Domains window. You can enter either a regular domain name or an IP address. If you specify a domain that does not exist, or enter *none*, then you effectively block access for this user.

   See Add Access Domain Window for a complete description of the contents of this window.

7. Click OK to add the domain to the list and dismiss the Add Access Domain window.

See POP/IMAP Delivery Window for a complete description of the contents of this window.

Specifying Program Delivery

Specifying this option provides a mechanism for forwarding messages to an external application for processing before delivery to the user.

> **Note:** This section describes only how to make the program delivery option available to an individual user. You must first enable the program delivery module as a whole, which requires performing several other administrative tasks. See Appendix B, Program Delivery, for details.

To enable program delivery for this user:

1. Access the Delivery Options form.
2. Check the Program delivery box, and click the Properties button to open the Program Delivery window.
3. Enter the external application command(s) to be used for processing this user's mail.
4. Click OK to submit your entry and dismiss the Program Delivery window.

See Program Delivery Window for a complete description of the contents of this window.

Specifying Unix Delivery

Specifying this option selects Unix delivery for this user. The Unix delivery feature allows messages to be delivered to the user's designated Unix mailbox. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

To enable Unix delivery for this user:

1. Access the Delivery Options form.
2. Check the Unix delivery box.

   Note: Beyond the steps shown here, providing Unix delivery to Messaging Server users naturally requires you to perform normal Unix mail administrative tasks.

Specifying Forwarding Addresses

The mail-forwarding feature of Messaging Server 4.0 enables a user's mail to be forwarded to another address instead of or in addition to the primary address for that user.

Messaging Server also provides an end-user HTML interface through which users can themselves specify forwarding addresses. The Netscape Console (administrator) interface and the HTML (user) interface both manipulate the same directory attributes; when opened, each shows the current settings, whether they were set by the administrator or by the user.

To specify forwarding-address information for a user:

1. In Netscape Console, access the Create User or Edit Entry window, as described in Accessing Mail Users.
2. Click the Mail tab.
3. Click the Forwarding tab. The Mail Forwarding form is displayed.

   The Forwarding Address field in the form shows the current set of forwarding addresses, if any, for the user.
4. To add a forwarding address, Click Add. The Add Forwarding Address window opens.
5. Enter a forwarding address in the Forwarding address field.
6. Click OK to add the address to the Forwarding address field in the Mail Forwarding form and dismiss the Add Forwarding Address window.

   (See Add Forwarding Address Window for a complete description of the contents of this window.)
7. Click OK in the Forwarding Address form if this action completes all changes that you wish to make to this user's mail information. Otherwise, click other tabs to continue making entries in other forms.

See Mail Forwarding Tab for a complete description of the contents of this form.

Configuring Auto-Reply Settings

The auto-reply feature of Messaging Server 4.0 allows you to specify an automatic response to incoming mail for a user. You can specify three different auto-reply modes: echo mode, vacation mode, and auto-reply mode.

Messaging Server also provides an end-user HTML interface through which users can themselves enable and configure auto-reply settings. The Netscape Console (administrator) interface and the HTML (user) interface both manipulate the same directory attributes; when opened, each shows the current settings, whether they were set by the administrator or by the user.

To enable an auto-reply service for a user:

1. In Netscape Console, access the Create User or Edit Entry window, as described in Accessing Mail Users.

2. Click the Mail tab.

3. Click the Auto-Reply tab. The Auto-reply form is displayed.

4. Select one of the auto-reply modes:

   Off: Disables auto-reply for this user.

   Echo: An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.

   Vacation: The first message received by this user from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, you can enter a reply message in the Message field.

   Auto-reply: Every incoming message received by the user generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the message field.

5. If you have selected echo, vacation, or auto-reply mode, you can (optionally) specify the reply message to be returned to the sender.You can crate one message in each of several available languages (specified in the popup menu above the field).

6. Click OK in the Auto-Reply form if this action completes all changes that you wish to make to this user's mail information. Otherwise, click other tabs to continue making entries in other forms.

See Auto-Reply Tab for a complete description of the contents of this form.

Managing Mailing Lists

Accessing Mailing Lists

This section describes how to get to the administration interface for your mailing lists. Because Messaging Server mailing lists are stored as attributes of group entries in an your enterprise's central LDAP user directory, managing mailing lists means accessing and modifying directory groups.

Creating a New Group

To create a new mailing list, you create a new group in the directory. You must also install a mail account for that group; if you do not install the mail account, the mail-administration portion of Netscape Console is not available. (The full process of creating a directory group and specifying other kinds of group information is described in more detail in *Managing Servers with Netscape Console*).

To create a new mailing list:

1. In the Netscape Console main window, click the Users and Groups tab. The Users and Groups window opens.

2. Select New Group and click Create. After you select an organizational unit for the group, the Create Group window opens (see Figure 4.4).

3. Enter at least the required information to create the group entry, as noted in the Users and Groups chapter of *Managing Servers with Netscape Console*.

   Note: For mailing-list purposes, you do *not* have to add members through the Members tab of the Users and Groups interface:

   - Mailing-list members have group privileges limited to those provided by the mailing-list component of the group (which may or may not be the only purpose for the group's existence). Mailing-list members are called *email-only members,* and you add them through the Mail tab.

   - Regular group members have full mailing-list privileges, but they also have to any other privileges that their group membership indicates. You add regular members through the Members tab.

4. Before closing the Create Group window, click the Account tab. A list of installable products for the group account appears in the right pane.

5. Click the Mail Account Install box. The Mail tab becomes visible in the Create Group window.

6. Click on the Mail tab in the Create Group window, then click the appropriate tab in the right pane to go to the desired form (see Figure 4.5). (These are the forms described in this chapter.)

7. Enter your changes, then click OK at the bottom of the Create Group window. This submits your entries and dismisses the Create Group window.

   Note. Clicking OK at the bottom of any mail administration form submits all of the current mail configuration information entered into all of the mail administration forms. Make sure you complete all setup procedures in the relevant forms before clicking OK.

Figure 4.4 Create Group window (without Mail tab)

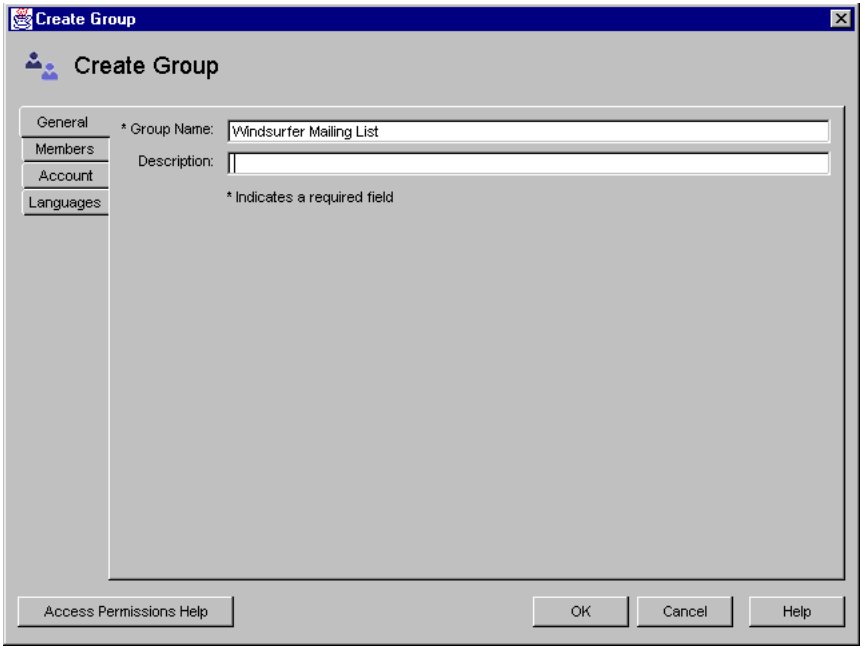
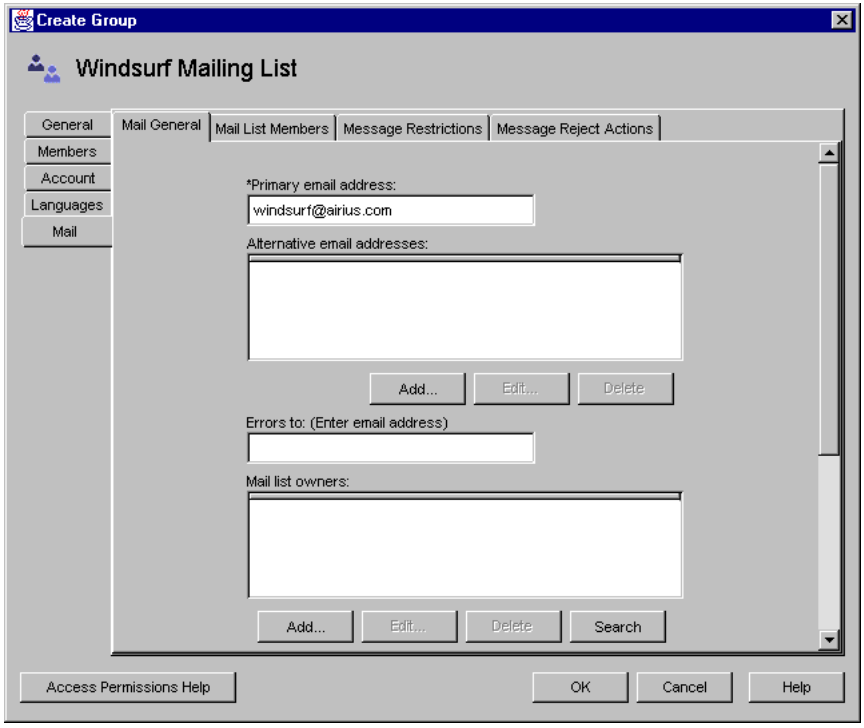


Figure 4.5 Create Group window with mail account installed (Mail tab selected)



Accessing an Existing Group

To modify an existing mailing list, or to add a mailing-list capabilities to an existing group, you access the appropriate group in the user directory and then add or modify it's mail-account attributes.

To access mailing-list information for an existing group:

1. In the Netscape Console main window, click the Users and Groups tab.
2. In the Users and Groups main window, Click Search or Advanced Search.
3. Enter your search criteria (such as the group's name) in the Search window, and perform the search of the user directory.
4. Back in the Users and Groups main window, select a group from the search results and click Edit. The Edit Entry window opens.

5. If the Mail tab is not visible in the Edit Entry window, do this:

   - Click the Account tab. A list of installable accounts appears in the right pane (see Figure 4.2).
   - Check the Mail Account Install box. The Mail tab now becomes visible in the Edit Entry window.

6. Click the Mail tab in the Edit Entry window, then click the appropriate tab in the right pane to go to the desired form.

   (These are the forms described in this chapter; they are identical to those you access through Create Group window.)

7. Enter your changes, then click OK at the bottom of the Edit Entry window. This submits your modifications and dismisses the Edit Entry window.

Specifying General List Information

Before mail can be delivered successfully to your mailing list, you must specify its mail-addressing information. This consists of the primary address for the group, any alternate addresses you want to accept as aliases to the primary address, plus optional descriptive information about the purpose, attributes, members, and so on, for the mailing list. This description is for informational purposes only; it is not used by the Messaging Server.

To specify general mailing-list information:

1. In Netscape Console, access the Create Group or Edit Entry window, as described in Accessing Mailing Lists.

2. Click the Mail tab.

3. Click the General tab, if it is not already frontmost. The Mail General form is displayed.

4. (Required) Enter the mailing list's primary email address.

   This is the publicized address to which this list's mail is to be delivered. There can be only one primary address for a list. It must be a correctly-formatted SMTP address that conforms to RFC 821 specifications.

5. (Optional) Click Add below the "Alternative email addresses" field to specify an alternate address for the mailing list. The Add Alternate Address window opens.

   - Enter an alternate address. An alternate address is an alias for the group's primary address. You can add as many alternate addresses to the list as you like, but you must explicitly open this window and add a single address each time.
   - Click OK in the Alternate Address window to add the address to the list and dismiss the window.

   (See Add/Edit Alternate Address Window for a complete description of the contents of this window.)

6. (Optional) Enter the email address of a person, if any, to whom errors in posting messages to the list should be sent.

7. (Optional) Click Add below the "Mail list owners" field to specify one or more owners of this list.

   The Add List Owners window opens. Click either DN or email address, enter the information in the window, then click OK to add the owner to the list and dismiss the window.

8. (Optional) Enter the host name of the machine hosting this mailing list.

   If the Primary email address field for this mailing list includes a host name, you can leave this field blank. If you implement host-name hiding by having no host name in the primary email address, specify the host name in this field.

9. (Optional) Enter a text description of the purpose or nature of the mailing list.

10. (Optional) Enter a URL to an HTML page providing additional information about the mailing list. This is for informational purposes only; the URL is not used by Messaging Server.

11. Click OK in the Mail General form if this action completes all changes that you wish to make to this mailing list. Otherwise, click other tabs to continue making entries in other forms.

See Mail General Tab for a complete description of the contents of this window.

Specifying List Members

You can add members to your mailing list by using one or both of the following methods:

- You can explicitly add each member to the mailing list.
- You can define dynamic criteria to be applied to the user directory as a filter for determining group membership.

The mailing-list members described here are called *email-only members* in the Users and Groups interface of Netscape Console, because they have group privileges limited to those provided by the mailing-list component of the group. "Regular" group members, which you add using a different part of the interface (described in *Managing Servers with Netscape Console*), may have additional privileges or responsibilities beyond those of mailing-list members.

Defining Dynamic Membership Criteria

Dynamic criteria consist of LDAP Search URLs that are used as filters in searching the user directory for determining membership. This mechanism is dynamic in that, when a message arrives for the group, the individuals that receive it are determined by a directory search rather than by consulting a static list of names. You can thus create and maintain very large or complex groups without having to track each member explicitly.

LDAP Search filters must be formatted in LDAP URL syntax. For more detailed information on constructing LDAP filters, see the users and groups chapter of *Managing Servers with Netscape Console*. See also the Directory Server documentation and RFC 1959.

An LDAP URL has the following syntax:

`ldap://`*`hostname`*`:`*`port`*`/`*`base_dn`*`?`*`attributes`*`?`*`scope`*`?`*`filter`*

where the elements of the URL have the following meanings:

Element	Description
hostname	Hostname of the Directory Server.
port	Port number for the LDAP server. If no port is specified, the standard LDAP port (389) is used.
base_dn	Distinguished name of an entry in the directory, to be used as the search base. This component is required.
attributes	The attributes to be returned. If no attributes are specified, all attributes are returned.
scope	Scope of search: • A scope of `base` retrieves information only on the search base (*base_dn*) itself. • A scope of `one` retrieves information one level below the search base (the search-base level is not included. • A scope of `sub` retrieves information on the search base and all entries below the search base.
filter	Search filter to apply to entries within specified scope of search. If no filter is specified, (`objectclass=*`) is used.

The following is an example of an LDAP Search URL that filters for users who have sunnyvale as their mail host:

```
ldap:///o=Airius Corp,c=US??sub?(&(mailHost=sunnyvale.ace.com)\
(objectClass=inetOrgPerson))
```

This URL filters for users who are members of the organization (`o`) of `Airius`, have the country (`c`) attribute of US, and a mail host (`mailHost`) of `sunnyvale`. The `objectClass` attribute defines the type of entry for which to search, in this case `inetOrgPerson`.

Note that, by default, group names found by a search are ignored; that is, their members are not considered to be part the group defined by the search.

As noted in the next section, Netscape Console provides a template window (the Construct LDAP Search URL window) that you can use as an aid in building a search URL.

Adding Mailing-List Members

To add (email-only) members to a mailing list:

1. In Netscape Console, access the Create Group or Edit Entry window, as described in Accessing Mailing Lists.

2. Click the Mail tab.

3. Click the Mail List Members tab. The Mail List Members form is displayed.

4. (Optional) To specify an LDAP Search URL for determining membership, click Add below the "Dynamic criteria for email-only membership" field. The Add Dynamic Criterion window opens.

   - Enter an LDAP Search URL in the field. For instructions on creating an LDAP Search URL, see Defining Dynamic Membership Criteria.

   - To create the URL, you can optionally click the Construct button to open the Construct LDAP Search URL window, a template that aids construction of the search URL.

   - Click OK to add your entry to the "Dynamic criteria for email-only membership" field and dismiss the Add Dynamic Criterion window.

   (See Add/Edit Dynamic Criterion Window for a complete description of the contents of this window.)

5. (Optional) To explicitly add an individual member to the mailing list, click Add below the "Members with Email Only Membership" field. The Add Email-Only Member window opens.

   - Enter the primary address for the new member in the field. It must be a correctly-formatted SMTP address that conforms to RFC 821 specifications. You should not enter an alternate address—especially if you specify restrictions for the group. You can add only one new member each time you open this window; the field cannot hold more than one address.

   - Click OK to add the user to the members list and dismiss the Add Email-Only Member window.

(See Add/Edit Email-Only Member Window for a complete description of the contents of this window.)

6. Click OK in the Mail List Members form if this action completes all changes that you wish to make to this mailing list. Otherwise, click other tabs to continue making entries in other forms.

See Mail List Members Tab for a complete description of the contents of this form.

Defining Message-Posting Restrictions

You can impose various kinds of restrictions on messages sent to a mailing list. You can define the set of people allowed to post messages, you can require authentication of senders, you can restrict where posted messages can come from, and you can limit the size of a posted message. Messages that violate the restrictions are rejected.

Note: Although these restrictions are useful for controlling several aspects of the incoming messages for a group, they are not intended to provide high-security access control.

To define message-posting restrictions for a group:

1. In Netscape Console, access the Create Group or Edit Entry window, as described in Accessing Mailing Lists.
2. Click the Mail tab.
3. Click the Message Restrictions tab. The Message Restrictions form is displayed.
4. (Optional) Define the allowed senders. Make one of the following choices:
   - **Anyone:** No restrictions on senders. (This is the default.)
   - **Anyone in the mailing list:** Only mailing-list members (plus group members that aren't email-only members) can post messages.

- **Anyone in the following list:** Only those users explicitly listed in the following field can post messages.

If you choose "Anyone in the following list," click Add below the Allowed Senders field to add a sender. The Add Allowed Sender window opens. Enter the email address or distinguished name (DN) of the allowed sender into the field. You can enter the address or DN directly, or you can click Find to open the Search Users and Groups window. Click OK to add the sender to the Allowed Senders field and dismiss the Add Allowed Sender window. Repeat this step for all other allowed senders you want to add.

(See Add/Edit Allowed Sender Window for a complete description of the contents of this window. See *Managing Servers with Netscape Console* for a description of the Search Users and Groups window.)

5. (Optional) Define the sender authentication policy. Make one of these choices:

   - **No special requirement:** Senders do not have to be authenticated. (This is the default.)
   - **Only allow senders with SMTP authentication:** Only those senders that have authenticated to their SMTP server can post messages. See SMTP Password Login for information on authenticated SMTP.
   - **Only allow messages with the following password:** Only messages that include the proper password are accepted.

   If you choose "Only allow messages with the following password," you can set up (or change) the password for message authentication by entering it (twice) into the fields below the button. Then, only messages that include that password will be accepted.

6. (Optional) Define the allowed sender domains, to restrict where senders can post messages from. Click Add below the Allowed sender domains field. The Add Allowed Sender Domain window opens. Enter a domain name, and click OK to add the domain to the list and dismiss the Add Allowed Sender Domain window.

   (See Add/Edit Allowed Sender Domain Window for a complete description of the contents of this window.)

7. (Optional) Define the maximum permitted message size. Enter the size (in bytes) into the field.

8. Click OK in the Message Restrictions form if this action completes all changes that you wish to make to this mailing list. Otherwise, click other tabs to continue making entries in other forms.

See Message Restrictions Tab for a complete description of the contents of this form.

Defining Message-Rejection Actions

You can specify that Messaging Server automatically execute certain notification actions when messages to your mailing list are rejected because they violate the list's message-posting restrictions.

This feature lets you to define the action to be executed upon rejection of a mail message, and to specify group moderators. The actions that the server can take include notification to a moderator and reply to the sender (with or without appending the original message).

To define message-rejection actions for a mailing list:

1. In Netscape Console, access the Create Group or Edit Entry window, as described in Accessing Mailing Lists.

2. Click the Mail tab.

3. Click the Message Reject Actions tab. The Message Reject Actions form is displayed.

4. (Optional) To automatically forward rejected messages to moderators, check the "Send message to the moderator(s)" box.

   The moderator or moderators then decides how to process the message. That may include approving the message and forwarding it back to the list (perhaps with a password). By checking this box you can thus institute a fully moderated mailing list.

   - If you need to define a moderator or moderators, click Add below the List moderators field to open the Add Moderator window.

- Enter the moderator's primary email address or distinguished name (DN) in the field. You can enter the address explicitly or you can click on Find to use the Search Users and Groups window. Note that you can add only one moderator each time you open the Add Moderator window.

- Click OK to add the moderator to the List Moderators list and dismiss the Add Moderator window.

(See Add/Edit Moderator Window for a complete description of the contents of this window. See *Managing Servers with Netscape Console* for a description of the Search Users and Groups window.)

5. (Optional) To automatically reply to rejected messages, check the "Send the following reply to the sender" box.

   - Enter the text of the reply message in the Reply text field. (If you delete the contents of this field, Messaging Server uses a brief default message in the reply.)

   - If you want the original message to be returned to the sender (as a MIME attachment) along with the reply message, check the "Include original message with reply" box.

   Note: If neither the "Send the following reply to the sender" box nor the "Send message to the moderator(s)" box is checked, Messaging Server acts as if the "Send the following reply to the sender" box were checked.

6. Click OK in the Message Reject Actions form if this action completes all changes that you wish to make to this mailing list. Otherwise, click other tabs to continue making entries in other forms.

See Message Reject Actions Tab for a complete description of the contents of that form.

Interface Reference: Managing Mail Users

This section describes the Netscape Console interface elements that allow you to configure and manage the mail-related components of the user information stored in the LDAP user directory. See *Managing Servers With Netscape Console*

for general information on using Netscape Console to manage Messaging Server and other servers. See *Directory Server Administrator's Guide* for information on LDAP, the user directory, and other user information stored in the directory.

Mail Settings Tab

You use the form accessed through this tab to define a user's Messaging Server host machine and email addresses.

For more information, see also Specifying User Email Addresses.

The Mail Settings form contains the following elements:

Messaging Server host name. In this field, enter the name of the Messaging Server that hosts this user's mail services. The host name you enter must be a fully-qualified domain name (FQDN). If the server has multiple host names, this must be the FQDN known to the Messaging Server on that machine.

Primary email address. in this field, enter the primary email address for this user. The primary address is the *publicized address*, the one displayed by address-book applications. Each user can have only one primary address.

The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications. Case is not significant; all characters that you enter in this field are forced to lower case.

> **Note.** If you want to implement host name hiding (the host name in the user's address is not to be shown in the outgoing mail header) do not specify the host name in the Primary email address field.

Alternate address. This field displays a list of this user's alternate email addresses, or aliases to the primary email address. Click the Add or Delete buttons to modify the information in this field.

Add. Click this button to open a window (see Add Alternate Address Window) that lets you add an address to the Alternate address field.

Delete. Click this button, after selecting an address in the Alternate address field, to remove that address from the user's list of alternate email addresses.

Action Buttons

OK. Click this button to commit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Mail Settings form.

Add Alternate Address Window

You use the Add Alternate Address window to define an alternate email address for a user and add it to the Alternate Address field in the Mail Settings form.

For more information, see also Specifying User Email Addresses.

The Add Alternate Address window contains the following elements:

Alternate email address for this user. In this field, enter the address to be added to the user's list of alternate email addresses.

Action Buttons

OK. Click this button to commit your changes and close the window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Add Alternate Address window.

Delivery Options Tab

You use the form accessed through this tab to configure the mail-delivery options available for a user.

For more information, see also

- Configuring Delivery Options

- Specifying Unix Delivery

The Delivery Options form contains the following elements:

POP/IMAP Delivery

Enable POP/IMAP delivery. Check this box to enable delivery to this user's regular POP3 or IMAP4 mailboxes. When the box is checked, the associated Properties button is active. Uncheck this box to disable POP/IMAP delivery.

Properties. If the "Enable POP/IMAP delivery" box is checked, click this button to open a window (see POP/IMAP Delivery Window) that lets you define various settings for POP/IMAP delivery for this user.

Program Delivery

Program delivery. Check this box to enable program delivery for this user. Program delivery can redirect the user's incoming mail to specified external commands, or applications. When this box is checked, the associated Properties button is active. Uncheck this box to disable program delivery for this user.

Checking this box makes program delivery available to the user only if it first has been enabled on your server. See Appendix B, Program Delivery, for details.

Properties. If the Program delivery box is checked, click this button to go a window (see Program Delivery Window) that lets you define the commands to be executed by this user's program delivery service.

Unix Delivery

Unix delivery. Check this box to enable standard Unix mail delivery as a delivery option for this user. When Unix delivery is activated for a user hosted by a Messaging Server running on a Unix host, incoming mail for the user is stored in the user's designated Unix mail file. Uncheck this box to disable Unix delivery.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Delivery Options form.

POP/IMAP Delivery Window

You use this window to configure delivery and access to an individual user's POP or IMAP mailboxes.

For more information, see also Specifying POP/IMAP Delivery

The POP/IMAP Delivery window contains the following elements:

Message store name. In this field, enter the name (nickname, not pathname) of the message store partition to which the user's incoming mail should be delivered, if other than the current default primary partition. The name must represent an existing partition. For information on the message store and instructions fore creating partition nicknames, see Chapter 5, Managing the Message Store.

Mail storage limit

Buttons in this area allow you to assign a disk quota, or allocated storage limit, specific to this user alone.

Use default. Click this button to set no specific limit on the amount of space in the message store allocated to this user.

> **Note:** If this button is selected, the user's storage limit is whatever is specified as the default disk quota for all users. For instructions on setting the default disk quota for the message store, see Configuring User Disk Quotas.

Limit to. Click this button to specify a disk quota for this user. Enter a number in the field and select the appropriate unit (KB or MB).

List of domains accessible to user for mail

Access domains. This field displays the list of domains from which the user can connect to the server to retrieve mail. Note these special cases:

- If no domains appear in this list, the user's access is unrestricted.
- If this list consists of the entry "none" or a nonexistent domain name, the user is effectively blocked from POP/IMAP logins to the server.

Use the Add button to add entries to this field; use the Delete button to delete entries.

Add. Click this button to open a window (see Add Access Domain Window) that lets you add an access domain to the Access domains field.

Delete. Click this button, after selecting an item in the Access domains field, to remove the item from this user's list of access domains.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the POP/IMAP Delivery window.

Add Access Domain Window

You use the Add Access Domain window to add a domain to the Access domain field in the POP/IMAP Delivery window.

For more information, see also Specifying POP/IMAP Delivery.

The Add Access Domain window contains the following elements:

Access domain name. In this field, enter the name of a domain from which this user has permission to access messages. The name you enter here is added to the list of domains in the Access domains field of the POP/IMAP Delivery window. You can enter either a regular domain name or an IP address.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Add Access Domain window.

Program Delivery Window

You use the Program Delivery window to define the commands to be executed for Program Delivery services.

For more information, see also

- Specifying Program Delivery
- Appendix B, Program Delivery

The Program Delivery window contains the following elements:

Program delivery command(s). Enter the command to be executed for program delivery services for this user.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Program Delivery window.

Mail Forwarding Tab

You use the form accessed through this tab to define forwarding addresses for a user.

For more information, see also Specifying Forwarding Addresses.

The Mail Forwarding form contains the following elements:

Forwarding address. This field displays the list of addresses to which the user's mail should be redirected when forwarding is enabled. Use the Add button to add addresses to this field; use the Delete button to remove addresses.

Add. Click this button to open a window (see Add Forwarding Address Window) that lets you add a forwarding address to the list of forwarding addresses for this user.

Delete. Click this button, after selecting an address in the Forwarding address field, to remove the selected item from the user's list of forwarding addresses.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Mail Forwarding form.

Add Forwarding Address Window

You use the Add Forwarding Address window to add a mail forwarding address to the Forwarding address list in the Mail Forwarding form.

For more information, see also Specifying Forwarding Addresses.

The Add Forwarding Address window contains the following elements:

Forwarding address. In this field, enter the forwarding address you want to add to the user's list of mail-forwarding addresses.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Add Forwarding Address window.

Auto-Reply Tab

You use the form accessed through this tab to enable or disable several kinds of automatic mail reply for a user, and to specify the contents of the response message.

For more information, see also Configuring Auto-Reply Settings.

The Auto-Reply form contains the following elements:

Auto-Reply Mode

Off . Click this button to disable all auto-reply modes for this user.

Echo. Click this button to enable echo mode. In echo mode, an automatic reply is sent for each received message, with the received message appended as a MIME attachment. If you select this mode, you can enter a reply message in the Reply text field.

Vacation. Click this button to enable vacation mode. In vacation mode, the first message received by this user from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, you can enter a reply message in the Reply text field.

Autoreply. Click this button to enable basic auto-reply mode. In auto-reply mode, every incoming message received by the user generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Reply text field.

Reply text. If you have selected the Echo, Vacation, or Autoreply buttons, you can use this filed to specify a reply message to be automatically returned to senders of messages to this user.

First specify the language in the language popup menu, then write the message in the text field. You can create more than one message; each language can have its own message.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Mail Auto-Reply form.

Interface Reference: Managing Mailing Lists

This section describes the Netscape Console interface elements that allow you to configure and manage the mail-related components of the groups defined in the LDAP user directory. See *Managing Servers With Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers. See *Directory Server Administrator's Guide* for information on LDAP, the user directory, and other group information stored in the directory.

Mail General Tab

You use the form accessed through this tab to specify basic information---such as the email addresses, mailing-list owners, and descriptive comments--for the mailing-list portion of a group.

For more information, see also

- Specifying General List Information
- Users and Groups chapter of *Managing Servers with Netscape Console* (for using the Search Users and Groups window)

  Note: The Mail General form contains a large number of elements. If the lower portion of the form is obscured when you first access it, use the scroll bar on the right side to view the remainder of the form.

The Mail General form contains the following elements:

Primary Address

Primary email address. In this field, enter the primary email address for this mailing list. The primary address is the publicized address, the one displayed by address-book applications. Each mailing list can have only one primary address. This information is required.

The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications.

> **Note.** If you want to implement host name hiding (the host name in the group's address is not to be shown in the outgoing mail header) do not specify the host name in the Primary email address field.

Alternate Addresses

Alternative email addresses. *This field displays a list of alternate email addresses for this mailing list. You can use this, for example, to ensure proper delivery of misaddressed mail (e.g., to correct for common misspellings) or to implement group host name hiding for outgoing message headers. You can add as many alternate addresses to the list as you like, provided each is unique.

Click the Add, Edit, or Delete buttons to modify the information in this field.

Add. Click this button to open a window (see Add/Edit Alternate Address Window) that lets you add an address to the Alternate email addresses field.

Edit. After selecting an address in the Alternative email addresses field, click this button to open a window (see Add/Edit Alternate Address Window) that lets you edit that alternate address.

Delete. After selecting an address in the Alternative email addresses field, click this button to remove the selected address from the field.

Error Address

Errors to. In this field, enter the email address of the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list bounces.

List Owners

Mail list owners. This field contains the distinguished names (DNs) of the owners of this mailing list. The list owner (or owners) typically created the mailing list, and has administrative privileges for adding or removing users, modifying configuration settings, or deleting the list.

Click the Add, Edit, Delete, or Search buttons to modify the information in this field.

Add. Click this button to open a window (see Add/Edit List Owner Window) that lets you add the distinguished name (DN) of an owner to the Mail list owners field.

Edit. After selecting an item in the Mail list owners field, click this button to open a window (see Add/Edit List Owner Window) that lets you edit that owner's DN.

Delete. After selecting a DN in the Mail list owners field, click this button to remove the selected owner from the field.

Search. Click this button to open the Search Users and Groups window, which lets you search the user directory for an owner that you can add to the Mail list owners field. (User and Group searching is described in *Managing Servers with Netscape Console*.)

Host

Messaging Server host name. In this field, enter the name of the Messaging Server that handles mail for this mailing list. The host name you enter must be a fully-qualified domain name (FQDN). If the server has multiple host names, this must be the FQDN known to the Messaging Server on that machine.

Leave this field blank if you want to allow any Messaging Server host to handle mail for the mailing list.

Information

Descriptive comments. In this field, enter any comments or descriptive notes pertaining to the mailing list.

URL for additional information. If you have created an HTML page or pages that give more information about this mailing list, enter the URL to that page here.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Mail General form.

Add/Edit Alternate Address Window

You use the Add/Edit Alternate Address window to add an address to, or edit an address in, the Alternate email addresses field in the Mail General form.

For more information, see also Specifying General List Information.

The Add/Edit Alternate Address window contains the following elements:

Enter alternative email address for the mailing list. Enter the address that you want to add, or edit the displayed address.

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Alternate Address window.

Add/Edit List Owner Window

You use the Add/Edit List Owner window to add or edit the distinguished name (DN) of a mailing list owner in the Mail list owners field in the Mail General form.

For more information, see also Specifying General List Information.

The Add/Edit List Owner window contains the following elements:

Enter list owner's DN. Enter the DN that you want to add, or edit the displayed DN. Note that you can use the Search button in the Mail General form to get the DN of an owner by searching the user directory.

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Alternate Address window.

Mail List Members Tab

You use the form accessed through this tab to view and modify the (email-only) membership of this mailing list. You can specify dynamic criteria for list membership, and you can also specify individual members by email address.

> **Important:** Mailing-list members defined here (email-only members) are different from other members of the directory group that this mailing list is part of. Group members entered through the Users and Groups interface (that is, through the Members tab rather than the Mail tab) are mailing-list members as well, but in addition have whatever other privileges the group (apart from its mailing list) may define.

For more information, see also Specifying List Members.

The Mail List Members form contains the following elements:

Dynamic criteria for email-only membership. This field displays the dynamic criteria, if any, that are used to define mailing-list membership. Dynamic criteria consist of LDAP search URLs, and could include specific user attributes such as organizational unit (for example, all employees in the Marketing organization) or Messaging Server host (for example, all users of the server `airiuspost1`). All users in the user directory matching any criteria defined here are considered members of this mailing list. Applying dynamic membership criteria saves you the effort of specifying each member explicitly when creating a mailing list.

Click the Add, Edit, or Delete buttons to modify the information in this field.

Add. Click this button to open a window (see Add/Edit Dynamic Criterion Window) that lets you add a dynamic membership criterion (in the form of an LDAP URL) to the "Dynamic criteria for email-only membership" field.

Edit. After selecting a criterion (LDAP URL) in the "Dynamic criteria for email-only membership" field, click this button to open a window (see Add/Edit Dynamic Criterion Window) that lets you edit the URL.

Delete. After selecting a criterion (LDAP URL) in the "Dynamic criteria for email-only membership" field, click this button to remove the criterion from the field.

Members with email-only membership. This field lists the email address of individual mailing-list members. You can specify members explicitly by placing their addresses in this field, instead of (or in addition to) defining membership with dynamic criteria. Group members that are not email-only members do not need to be listed in this field.

> **Note:** Because only an emil address is required, you can use this field to add members to the mailing list that do not appear in the LDAP user directory.

Click the Add, Edit, or Delete buttons to modify the information in this field.

Add. Click this button to open a window (see Add/Edit Email-Only Member Window) that lets you add a user to the "Members with email-only membership" field.

Edit. After selecting an item in the "Members with email-only membership" field, click this button to open a window (see Add/Edit Email-Only Member Window) that lets you edit that member's address.

Delete. After selecting an item in the "Members with email-only membership" field, click this button to remove the selected member from the list.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Mail List Members form.

Add/Edit Dynamic Criterion Window

You use the Add/Edit Dynamic Criterion window to specify an LDAP Search URL that can be used as a filter for dynamically defining mailing-list membership.

For more information, see also

- Defining Dynamic Membership Criteria
- Users and Groups chapter of *Managing Servers with Netscape Console* (for using the Construct LDAP URL window)

The Add/Edit Dynamic Criterion window contains the following elements:

Enter an LDAP search URL. In this field, enter the LDAP filter you want to add to the "Dynamic criteria for email-only membership" field of the Mail List Members form (or edit the existing filter that appears here). The result of your entry or edit must be a single, complete filter.

Construct. Click this button to open the Construct LDAP URL window, which provides a template you can use to construct your search filter. (The LDAP URL window is described in *Managing Servers with Netscape Console*.)

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Dynamic Criterion window.

Add/Edit Email-Only Member Window

You use the Add/Edit Email-Only Member window to add a user to the "Members with email only membership" field in the Mail List Members form.

For more information, see also Specifying List Members.

The Add/Edit Email-Only Member window contains the following elements:

Enter User's Email Address. In this field, enter the email address of the user you want to add to the "Members with email only membership" field in the Mail List Members form (or edit the existing address that appears here). The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications.

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Email-Only Member window.

Message Restrictions Tab

You use the form accessed through this tab to implement policies that govern who is allowed to send messages to this mailing list and how large the messages can be.

For more information, see also

- Defining Message-Posting Restrictions
- Users and Groups chapter of *Managing Servers with Netscape Console* (for using the Search Users and Groups window)

Note: The Message Restrictions form contains a large number of elements. If the lower portion of the form is obscured when you first access it, use the scroll bar on the right side to view the remainder of the form.

The Message Restrictions form contains the following elements:

Allowed Senders

Select one of the following three choices to specify who is allowed to post messages to the mailing list. (The default is "Anyone.")

Anyone. Click this button to remove all restrictions on senders.

Anyone in the mailing list. Click this button to restrict message-posters to mailing-list members only. (Group members that aren't email-only members will also be allowed to post.)

Anyone in the following list. Click this button to allow only those users that appear in the following field (Allowed Senders field) to be able to post messages to the mailing list.

The field contains either the email address or the distinguished name (DN) of a user. The field must contain at least one entry for this button to be selected.

> **Note:** If you want all list members *plus* other individuals to be allowed to post messages, put the DN or email address of the mailing list itself into this field, plus whatever other individuals you want to have posting permission.

Click the Add, Edit, Delete, or Search buttons to modify the content of this field.

Add. Click this button to open a window (see Add/Edit Allowed Sender Window) that lets you add a new user to the Allowed Senders field.

Edit. After selecting an item in the Allowed Senders field, click this button to open a window (see Add/Edit Allowed Sender Window) that lets you edit that sender's DN or email address.

Delete. After selecting an item the Allowed Senders field, click this button to remove the sender from the field.

Search. Click this button to open the Search Users and Groups window, which lets you search the user directory for a user that you can add to the Allowed Senders field. (User and Group searching is described in *Managing Servers with Netscape Console*.)

Sender Policy

Select one of the following three sender-authentication policies. (The default is "No special requirement.")

No special requirement. Click this button to require no authentication from senders.

Only allow senders with SMTP authentication. Click this button to accept messages from only those senders that have authenticated to their SMTP server. See SMTP Password Login for information on authenticated SMTP.

Only allow messages with the following password. *Click this button, and enter a password into the following fields, to define a password specific to this mailing list. Only messages whose headers include that password will be accepted.

If you select this option, you must enter a password.

Password. Enter the sender password for this mailing list.

Password. Re-enter the password for verification.

Sender Domains

Allowed sender domains. This fields displays the list of domains from which messages will be accepted for posting to this mailing list. If none is specified, there is no sender-domain restriction.

Click the Add, Edit, or Delete buttons to modify the information in this field.

Add. Click this button to open a window (see Add/Edit Allowed Sender Domain Window) that lets you add a domain to the Allowed Sender Domains field.

Edit. After selecting an item in the Allowed Sender Domains field, click this button to open a window (see Add/Edit Allowed Sender Domain Window) that lets you edit the domain specification.

Delete. After selecting an item in the Allowed Sender Domains field, click this button to remove the selected member from the field.

Maximum Message Size

Maximum message size (in bytes). Enter the maximum permitted size (in bytes) for messages to be posted to this mailing list.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Message Restrictions form.

Add/Edit Allowed Sender Window

You use the Add/Edit Allowed Sender window to add users to the Allowed Sender list in the Message Restrictions form, or to edit the information about an existing allowed sender. An allowed sender is a user with permission to post messages to a particular mail group.

For more information, see also Defining Message-Posting Restrictions.

The Add/Edit Allowed Sender window contains the following elements:

DN. Click this button if you are entering a distinguished name.

Email address. Click this button if you are entering an email address.

Enter sender's email address or DN. In this field, enter the email address or distinguished name of the user you want to add to the Allowed Sender list in the Message Restrictions form.

> **Note:** You can enter the DN or email address of a group in this field. If you do so, all members of that group become allowed senders.

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Allowed Sender window.

Add/Edit Allowed Sender Domain Window

You use the Add /Edit Allowed Sender Domain window to add a domain to the Allowed sender domains field of the Message Restrictions form, or to edit the specification of an existing allowed domain. An allowed domain is a domain from which incoming messages can be accepted for posting to this mailing list.

For more information, see also Defining Message-Posting Restrictions.

The Add/Edit Allowed User Domain window contains the following elements:

Enter a domain name. In this field, enter (or edit) the name of the domain you want to allow posting from. The result of your entry is placed in the Allowed sender domains field of the Message Restrictions form.

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add Allowed Sender Domain window.

Message Reject Actions Tab

You use the form accessed through this tab to define the action to be executed automatically upon rejection of mail messages that do not meet the message-restriction criteria defined in the Message Restrictions form.

For more information, see also

- Defining Message-Rejection Actions
- Users and Groups chapter of *Managing Servers with Netscape Console* (for using the Search Users and Groups window)

The Message Reject Actions window contains the following elements:

Message to Moderators

Send message to the moderator(s). Check this box to automatically forward rejected messages to the mailing-list moderator or moderators for further action. (Specifying this option does not preclude you from also specifying an automatic reply to the sender.) If you check this box, you must make at least one entry in the List moderators field.

List moderators. This field displays the list of moderators for this group. A moderator is specified either by email address or by distinguished name (DN). Click the Add, Edit, Delete, or Search buttons to modify the content of this field.

Add. Click this button to open a window (see Add/Edit Moderator Window) that lets you add a new moderator for this mailing list to the List moderators field.

Edit. After selecting an item in the List moderators field, click this button to open a window (see Add/Edit Moderator Window) that lets you edit the moderator's DN or email address.

Delete. After selecting an item the List moderators field, click this button to remove the moderator from the field.

Search. Click this button to open the Search Users and Groups window, which lets you search the user directory for a user that you can add to the List moderators field. (User and Group searching is described in *Managing Servers with Netscape Console*.)

Reply to Sender

Send the following reply to the sender. Check this box to automatically send a reply to the sender of any rejected message. (Specifying this option does not preclude you from also specifying that the list moderators be notified.)

This option is the default: if neither this box nor the "Send message to the moderator(s)" box is checked, Messaging Server behaves is if this box were checked.

Include original message with reply. If the "Send the following reply to the sender" box is checked, you can check this box to append the original rejected message as a MIME attachment to the automatic reply. Uncheck this box to send the reply only, without appending the original message.

Reply text. First select a language in the popup menu, then enter in this field the text to be used for the reply message. You can create a separate message for each language, so that senders can receive replies in their preferred language.

Messaging Server provides an initial default reply text string in the Reply text field. If you delete all text in that field, the server nevertheless includes a brief default message in the reply.

Action Buttons

OK. Click this button to submit your entries and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entries.

Help. Click this button to display online help (this document) that describes the Message Reject Actions form.

Add/Edit Moderator Window

You use the Add/Edit Moderator window to add a user to the List moderators field in the Message Reject Actions form.

For more information, see also Defining Message-Rejection Actions.

The Add/Edit Moderator window contains the following elements:

DN. Click this button if you are entering a distinguished name.

Email address. Click this button if you are entering an email address.

Enter moderator's DN or email address. In this field, enter the email address or distinguished name of the user you want to add to the list of moderators for the mailing list (or edit the information for an existing moderator).

Action Buttons

OK. Click this button to submit your entry and dismiss this window.

Cancel. Click this button to dismiss the window without submitting your entry.

Help. Click this button to display online help (this document) that describes the Add/Edit Moderator window.

Chapter

5

Managing the Message Store

This chapter describes the message store and the message store administration interface. This chapter contains the following sections:

- Overview
- Message Store Architecture
- How Messages Are Erased from the Store
- Specifying Administrator Access
- Configuring User Disk Quotas
- Configuring Message Store Partitions
- Specifying Aging Policies
- Performing Maintenance and Recovery Procedures
- Interface Reference: Message Store Configuration

Overview

The message store contains the user mailboxes for a particular Messaging Server instance. The size of the message store increases as the number of mailboxes, folders, and log files increase. You can control the size of the store by specifying limits on the size of mailboxes (disk quotas) and by setting aging policies for messages in the store.

As you add more users to your system, your disk storage requirements increase. Depending on the number of users your server supports, the message store might require one physical disk or multiple physical disks. If you have a very large user base, you might have multiple Messaging Server instances, each responsible for a particular message store.

To manage the message store, Netscape Messaging Server provides a set of command-line utilities in addition to the Netscape Console interface. Table 5.1 describes these command-line utilities. For information about using these utilities, see Performing Maintenance and Recovery Procedures and Appendix A, Command-line Utilities.

Table 5.1 Message store command-line utilities

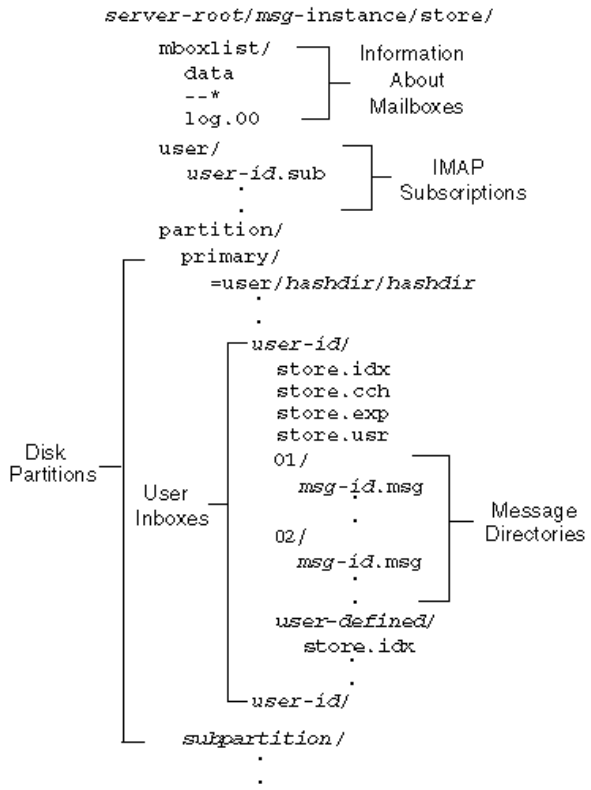
Utility	Description
`hashdir`	Identifies the directory that contains the message store for a particular user.
`mboxutil`	Lists, creates, deletes, renames, or moves mailboxes.
`quota`	Reports quota usage.
`readership`	Collects readership information on mailboxes.
`reconstruct`	Reconstructs mailboxes that have been damaged or corrupted.
`stored`	Performs background and daily tasks, expunges, and erases messages stored on disk.

Netscape Messaging Server also provides utilities to help you upgrade from a 3.x server to a 4.x server. For details about the upgrade process, see the server installation documentation.

Message Store Architecture

Figure 5.1 shows the message store architecture for a server instance. The message store is designed to provide fast searching of the store directories for improved server performance. The store directories are described in Table 5.2.

Figure 5.1 Message store architecture



For example, a sample directory path might be:

server-root/msg-*instance*/store/partition/primary/=user/53/53/=mack1/00

Table 5.2 Message store directories

Location	Content/Description
server-root/msg-*instance*/store/	Top-level directory of the message store. Contains the mboxlist, user, and partition subdirectories.
/store/mboxlist/	Contains the data and database support file directories. The mboxlist directory organizes data (found in other directories) so that it can be searched very quickly.
/store/mboxlist/data/	Contains information about quotas, quota usage, ACLs for the Messaging Server, and a copy of some of the information in store.idx. There is one entry for each account on the server. The data file is a Berkeley DB file.
/store/user/	Contains information about the IMAP folders to which each user subscribes. Information for each user is stored in a file called *user-id*.sub. These files are stored in a hash structure for fast searching. To find the directory that contains a particular user's files, use the hashdir utility.
/store/partition/	Contains the default primary partition and any subpartitions you define.
/*subpartition*/=user/	Contains all the user mailboxes in the subdirectory of the partition. The mailboxes are stored in a hash structure for fast searching. To find the directory that contains a particular user's mailbox, use the hashdir utility.
/=user/*hashdir/hashdir/user-id/*	The top-level mail folder for the user whose ID is *user-id*. Messages are delivered to this mail folder.
/user-id/folder-name	A user-defined folder.

Table 5.2 Message store directories

Location	Content/Description
*/user-id/*store.idx	An index that provides the following information about mail stored in the */user-id/* directory: number of messages, disk quota used by this folder, the time the index was last appended, and pointers to the store.cch file for each message. The index also includes a backup copy of mboxlist information for each user and a backup copy of quota information for each user.
*/user-id/*store.cch	A cache file for frequently requested message information. The file contains variable-length information for each message including caches of some headers and the MIME structure of messages. **Note:** The authenticated sender information in this file can be lost by running the reconstruct utility.
*/user-id/*store.exp	Contains a list of messages that will soon expire.
*/user-id/*store.usr	Contains a list of all messages that each user has seen, including information about the last time the user accessed the folder and which messages were deleted.
/user-id/nn/	A hash directory that contains messages in the format *msg-id*.msg; *nn* can be a number from 01 to *nn*.

How Messages Are Erased from the Store

Messages are erased in three stages:

1. **Delete**. An IMAP or POP client marks the message to be deleted. (IMAP clients use the `/deleted` flag; POP clients use the `DELE` command.) At this point, the client can restore the message by removing the "deleted" marking.

2. **Expunge**. A client, or the aging policies you have specified, expunges messages that have been marked deleted from the mailbox. (IMAP clients use the `EXPUNGE` command. POP clients use the `QUIT` command.) Once messages are expunged, the client can no longer restore them, but they are still stored on disk. (A second POP or IMAP client with an existing connection to the same mailbox may still be able to fetch the messages.)

3. **Cleanup**. The `stored` utility erases from the disk any messages that have been expunged for at least one hour.

Specifying Administrator Access

Message store administrators can view and monitor user mailboxes and specify access control for the store.

To specify administrator access to the store:

1. In the Messaging Server console, select the Configuration tab.

2. Open the Message Store folder.

   The message store configuration tabs appear in the right pane.

3. Click Administrator.

   The Administrator form appears.

From this form, you can perform the following tasks:

- Adding an Administrator
- Modifying an Administrator Entry

- Deleting an Administrator Entry

Adding an Administrator

To add an administrator entry:

1. Go to the Administrator form.

   The form contains a list of any existing administrator IDs.

2. Click the Add button beside the Administrator UID window.

3. In the Administrator UID field, type the user ID of the administrator you want to add.

   The user ID you type must be known to the Netscape Directory Server.

4. Click OK to add the administrator ID to the list displayed on the Administrator form.

5. Click Save on the Administrator form to save the newly modified Administrator list.

Modifying an Administrator Entry

To modify an existing entry in the message store Administrator UID list:

1. Go to the Administrator form.

2. Click the Edit button beside the Administrator UID window.

3. Enter your changes to the Administrator UID field.

4. Click OK to submit your changes and dismiss the Edit Administrator window.

5. Click Save on the Administrator form to submit and preserve the modified Administrator list.

Deleting an Administrator Entry

To delete an entry from the message store Administrator UID list:

1. Go to the Administrator form.
2. Select an item in the Administrator UID list.
3. Click Delete to delete the item.
4. Click Save to submit and preserve your changes to the Administrator list.

Configuring User Disk Quotas

You can specify disk quotas to control disk space usage. Disk quotas allow you to limit users to a fixed mailbox size. If disk space is limited, you might want to set user disk quotas.

If the size of a user's mailbox exceeds the specified limit, messages destined for the mailbox remain in the message queue until one of the following occurs: (1) The size no longer exceeds the limit, at which time the server delivers the message to the mailbox. (2) The message has been in the queue longer than the specified grace period and the user is still over quota, at which time the server bounces the message. Disk space becomes available when a user deletes and expunges messages or when the server deletes messages according to the maintenance policies you have established.

You can set disk quotas for individual users by using the Users and Groups interface. You can set default disk quotas for all users by choosing the Message Store Quota tab.

1. In the Messaging Server console, select the Configuration tab.
2. Open the Message Store folder.

   The message store configuration tabs appear in the right pane.
3. Click Quota.

   The Quota form appears.

From this form, you can perform the following tasks:

- Specifying a Default User Disk Quota
- Specifying a Quota Threshold
- Defining a Quota Warning Message
- Setting a Grace Period

Specifying a Default User Disk Quota

The default disk quota applies to all users who do not already have individual disk quotas set for them. A quota set for an individual user overrides the default quota.

1. Go to the Message Store Quota form.
2. Select one of the following options:
    - Unlimited. Select this option if you do not want to set a default disk quota.
    - Size specification. Select this option if you want to restrict the default user disk quota to a specific size. In the field beside the button, type a number, and from the pulldown menu, choose Mbytes or Kbytes.
3. Click Save.

Specifying a Quota Threshold

You can send a warning message to users before they reach their disk quota by specifying a quota threshold. When a user's disk usage exceeds the specified threshold, the server sends a warning message to the user.

For IMAP users whose clients support the IMAP ALERT mechanism, the message is displayed on the user's screen each time the user makes an IMAP connection (a message is also written to the IMAP log). For POP users and for IMAP users whose client does not support the IMAP ALERT mechanism, a message is stored in the user's inbox.

To specify a quota threshold:

1. Go to the Message Store Quota form.
2. In the "Quota warning threshold" field, enter a number for the warning threshold.

   This number represents a percentage of the allowed quota. For example, if you specify 90%, the user is warned after using 90% of the allowed disk quota. The default is 90%. To turn off this feature, enter 100%.
3. Click Save.

Defining a Quota Warning Message

You can define the message that will be sent to users who have exceeded their disk quota as follows. Messages are sent to the user's mailbox.

1. Go to the Message Store Quota form.
2. From the pull-down menu, choose the language you want to use.
3. Type the message you want to send in the message text field below the Threshold field.
4. Click Save.

Setting a Grace Period

If a user mailbox exceeds the disk quota, the grace period you specify determines how long messages will be held in the SMTP queue before the server starts bouncing the messages. Messages will remain in the queue until one of the following occurs: (1) The mailbox no longer exceeds the quota, at which time the server will deliver the message to the mailbox; (2) The message has remained in the queue longer than the specified grace period, at which time the server will bounce the message.

To set a grace period for how long messages are held in the queue:

1. Go to the Message Store Quota form.
2. In the "Over quota grace period" field, enter a number.
3. From the pulldown menu, specify Day(s) or Hour(s).
4. Click Save.

Configuring Message Store Partitions

All user mailboxes are stored by default in the `/store/partition/`directory. The `partition` directory is a logical directory that might contain a single subpartition or multiple subpartitions. The subpartitions might map to a single physical drive or to multiple physical drives. At start-up time, the `partition` directory contains one subpartition called the `primary` partition.

You can add partitions to the `partition` directory as necessary. For example, you might want to partition a single disk to organize your users as follows:

- `/partition/mkting/`
- `/partition/eng/`
- `/partition/sales/`

As disk storage requirements increase, you might want to map these partitions to different physical disk drives.

You should limit the number of mailboxes on any one disk. Distributing mailboxes across disks improves message delivery time (although it does not necessarily change the SMTP accept rate). The number of mailboxes you allocate per disk depends on the disk capacity and the amount of disk space allocated to each user. For example, you can allocate more mailboxes per disk if you allocate less disk space per user.

If your message store requires multiple disks, you can use RAID (Redundant Array of Inexpensive Disks) technology to ease management of multiple disks. With RAID technology, you can spread data across a series of disks but the disks appear as one logical volume so disk management is simplified. You might also want to use RAID technology for redundancy purposes; that is, to duplicate the store for failure recovery purposes.

To add a partition to the store, do the following:

1. In the Messaging Server console, select the Configuration tab.
2. Open the Message Store folder.

   The message store configuration tabs appear in the right pane.
3. Click Partition. The Message Store Partition form appears.
4. Click the Add button.
5. Enter the Partition nickname.

   The name you enter must be an alphanumeric name and must use lowercase letters.

   The partition nickname allows you to map users to a logical partition name regardless of the physical path. When setting up user accounts and specifying the message store for a user, you can use the partition nickname.
6. Enter the Partition path.

   This is the absolute pathname for the specified partition. The partition will be created at this location. The user ID used to run the server must have permission to write to this location, in order to create and manage the partition.
7. To specify this as the default partition, click the selection box labeled Make This the Default Partition.
8. Click OK to submit this partition configuration entry and dismiss the window.
9. Click Save to submit and preserve the current Partition list.

Important: After adding a partition, you must stop then restart the server to refresh the configuration information.

Note: To improve disk access, the message store and the message queue should reside on separate disks.

Specifying Aging Policies

Aging policies are another way to control disk usage on your server. You can control how long messages are stored in one or more mailboxes. If you have limited disk space, you might want to set aging policies for the store. If you set aging policies, you should educate your users about these policies because the server will not send a warning message before it starts deleting messages from the store.

You can create aging rules based on the following criteria:

- Number of messages in the mailbox
- Total size of the mailbox
- Number of days that messages remain in the mailbox
- Number of days that messages exceeding a given size remain in the mailbox

If you specify more than one rule for a mailbox, all expiration rules will apply, but the most restrictive rule takes precedence. For example, assume two rules apply to a single mailbox. The first rule allows 1000 messages; the second rule allows 500 messages. When expiration occurs, the server will delete messages from the mailbox until 500 remain. For another example, if the first rule allows a message size of 100,000 bytes for 3 days and the second rule allows a message size of 1000 bytes for 12 days, the resulting union of rules allows a message size of 1000 bytes for 3 days. The server will delete messages over 1000 bytes that have been in the mailbox over 3 days. If you want to ensure that a specific rule is the only rule for a particular mailbox or set of mailboxes, use the Exclusive parameter.

To create a new rule:

1. In the Messaging Server console, select the Configuration tab.
2. Open the Message Store folder.

   The message store configuration tabs appear in the right pane.
3. Click Aging. The Message Store Aging form appears.
4. Click Add to go to the Add Rule window.
5. Enter a name for the new rule.

6. Specify the target folders for which this rule applies.

   You can enter a pathname, filename, or partial string. You can use IMAP wildcards as follows:

   * Match any character.
   % Match any character except a slash character.

   The new rule applies only to folders matching the pattern you specify.

7. If this rule is to be the only rule applied to the target folders, click the Exclusive selection box.

8. If you want to create a rule based on folder size, do the following:

   - In the "Message count" field, specify the maximum number of messages which will be retained in a folder before the oldest messages are removed.

   - In the "Folder size" field, specify a number for the folder size and choose Mbyte(s) or KByte(s) from the pull-down menu.

   When the specified folder size is exceeded, the server removes the oldest messages until this size is no longer exceeded.

9. If you want to create a rule based on message age, in the "Number of days" field, specify a number to indicate how long messages should remain in the folder.

10. If you want to create a rule based on message size:

    - In the "Message size limit" field, enter a number to indicate the maximum size message allowed in the folder and choose Mbytes or Kbytes from the pulldown menu.

    - In the "Grace period" field, enter a number to indicate how long over-sized messages should remain in the folder.

    After the grace period, the server deletes messages that exceed the maximum size.

11. Click OK to add the new rule to the Aging Rule list and dismiss the Add window.

12. Click Save to submit and preserve the current Aging Rule list.

Performing Maintenance and Recovery Procedures

This section provides information about the utilities you use to perform maintenance and recovery tasks for the message store. You should always read your postmaster mail for warnings and alerts that the server might send. You should also monitor the log files for information about how the server is performing.

You can configure the server error handler so that error messages about disk quota are sent to the postmaster account and to the log file. For more information about configuring the error handler, see Chapter 3, Configuring SMTP Services. For more information about log files, see Chapter 11, Logging and Log Analysis.

Using the stored Utility

The `stored` utility performs the following monitoring and maintenance tasks for the server. This utility automatically performs cleanup and expiration operations once a day.

- background and daily messaging tasks
- low-level database consistency check and repair
- deadlock detection and rollback of deadlocked database transactions
- cleanup
- expiration, expunging, and erasing messages stored on disk
- alarm setting

Table 5.3 lists the `stored` syntax options. For more information, see Appendix A, Command-line Utilities.

Table 5.3 stored syntax options

Option	Description
`-c`	Performs one cleanup pass to erase expunged messages. Runs once, then exits. The `-c` option is a one-time operation, so you do not need to specify the `-1` option.
`-d`	Run as daemon. Performs system checks and activates alarms, deadlock detection, and database repair.
`-h` *`hour`*	Run once each day to perform cleanup and expiration operations. The *`hour`* value designates the hour of the day that `stored` is to automatically run. Specify *`hour`* in 24 hour format. For example `23` means 11pm. You do not need to use the `-1` option when using `-h`.
`-1`	Run once, then exit.
`-n`	Run in trial mode only. Does not actually expire or cleanup messages. Runs once, then exits.
`-v`	Verbose output.
`-v -v`	More verbose output.

You can set up `stored` to perform an additional cleanup and expiration operation at a specified hour. For example, to run stored as a daemon once a day at 9:00 p.m., use the following command:

```
stored -d -h 21
```

Occasionally, you might need to restart the `stored` utility; for example, if the mailbox list database becomes corrupted. To restart `stored`, use the following commands at the command line:

```
/etc/NscpMsg stop store
/etc/NscpMsg start store
```

If any server daemon crashes, you should restart all daemons including `stored`.

Managing Mailboxes

The mailboxes in the message store are stored in a hash structure for fast searching. Consequently, to find the directory that contains a particular user's mailbox, use the `hashdir` utility as follows:

```
hashdir userid
```

You use the `mboxutil` command to perform typical maintenance tasks on mailboxes. These tasks include the following:

- list mailboxes
- create mailboxes
- delete mailboxes
- rename mailboxes
- move mailboxes

Table 5.4 lists the `mboxutil` syntax options. For more information on using the `mboxutil` command, see Appendix A, Command-line Utilities.

Table 5.4 mboxutil options

Option	Description
`-c mailbox`	Creates the specified mailbox.
`-d mailbox`	Deletes the specified mailbox.
`-l`	Lists all of the mailboxes on a server.
`-p pattern`	When used in conjunction with the `-l` option, lists only those mailboxes with names that begin with the letters specified by *`pattern`*. You can use IMAP wildcards.
`-r oldname newname [partition]`	Renames the mailbox from *`oldname`* to *`newname`*. To move a folder from one partition to another, specify the new partition with the *`partition`* option.
`-x`	When used in conjunction with the `-l` option, shows the path and access control for a mailbox.

You must specify mailbox names in the following format: `user/`*`userid`*`/`*`mailbox`*, where *`userid`* it the user that owns the mailbox and `mailbox` is the name of the mailbox. For example, the following command creates a mailbox named INBOX for the user whose user ID is crowe:

```
mboxutil -c user/crowe/INBOX
```

Repairing Mailboxes and the Mailboxes Database

If one or more mailboxes becomes corrupt, you can use the `reconstruct` utility to rebuild the mailboxes or the mailboxes database, and repair any inconsistencies. Table 5.5 lists the syntax options for the `reconstruct` utility. For more information about using the `reconstruct` command, see Appendix A, Command-line Utilities.

Table 5.5 reconstruct options

Option	Description
`-m`	Performs a high-level consistency check and repair of the mailboxes database. This option assumes that `stored` is running. This option examines every mailbox it finds in the spool area, adding or removing entries from the mailboxes database as appropriate. The utility prints a message to the standard output file whenever it adds or removes an entry from the database.You can run this option while other server processes are running.
`-p` *`partition`*	Specifies a partition name. You can use this option on the first usage of *`reconstruct`*.
`-q`	Fixes any inconsistencies in the quota subsystem, such as mailboxes with the wrong quota root or quota roots with the wrong quota usage reported.
`-r [`*`mailbox`*`]`	Performs a consistency check and repairs the partition area of the specified mailbox or mailboxes. The `-r` option also repairs all sub-mailboxes within the specified mailbox. If you specify `-r` with no mailbox argument, the utility repairs the spool areas of all mailboxes within the database. You can run this option while other server processes are running.

To perform a high-level consistency check and repair of the mailboxes database, use the `-m` option.

```
reconstruct -m
```

For example, you should use the `-m` option when:

- One or more directories were removed from the message store, so the mailbox database entries need to be removed.
- One or more directories were restored to the message store, so the mailbox database entries need to be added.
- If the low-level database check and repair performed the `stored` process are not sufficient.

To rebuild mailboxes, use the `-r` option. For example, to rebuild the spool area for the mailboxes belonging to the user daphne, use the following command:

```
reconstruct -r user/daphne
```

Depending on the size of your message store, you should try to avoid using the `-r` option to rebuild the spool area for all mailboxes listed in the mailbox database. Running the `-r` option can take a very long time for large message stores. A better method for failure recovery might be to use multiple disks for the store. If one disk goes down, the entire store does not. If a disk become corrupt, you need only rebuild a portion of the store by using the `-p` option as follows:

```
reconstruct -p subpartition
```

Monitoring Disk Space

You can monitor disk space by configuring the following alarm attributes. You configure these attributes by using the `configutil` utility. You can specify how often the system should monitor disk space and under what circumstances the system should send a warning.

```
alarm.diskavailmsgalarmstatinterval
alarm.diskavail.msgalarmthreshold
alarm.diskavail.msgalarmwarninginterval
```

For example, if you want the system to monitor disk space every 600 seconds, specify the following command:

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

If you want to receive a warning whenever available disk space falls below 20 %, specify the following command:

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

For more information about setting alarm attributes, see Appendix A, Command-line Utilities.

Monitoring Disk Quota Usage

You can monitor disk quota usage by using the `quota` utility. The `quota` generates a report that lists defined quotas and limits, and provides information on quota usage. For more information on the `quota` utility, see Appendix A, Command-line Utilities.

Backing Up and Restoring the Message Store

For information about backing up the message store and restoring the message store, contact your Netscape technical support person.

Interface Reference: Message Store Configuration

This section describes the Messaging Server interface elements that allow you to configure the server's message store services. You access these elements through Netscape Console; see *Managing Servers With Netscape Console* for information on using Netscape Console to manage the Messaging Server and other Netscape servers.

Administrator Tab

You use the form accessed through the Message Store Administrator tab to view the list of message store administrators and to add entries to this list. For more information, see also: Specifying Administrator Access.

Administrator UID list. This area displays the list of administrators for this message store.

Add. Click this button to go to the Add Administrator window. This window enables you to add administrators to the list.

Edit. Click this button to go to the Edit Administrator window. This window enables you to edit the selected entry in the Administrator UID list.

Save. Click this button to save the current administrator list.

Reset. Click this button to return the list contents to the last saved version.

Help. Click this button to go to the Online Help window for this topic.

Add/Edit Administrator Window

The Add Administrator and Edit Administrator windows are identical. These windows enable you to add or edit an entry in the message store administrator list.

Administrator UID. In this field, enter the user ID of the Administrator you want to add to the message store administrator list. This must be a valid user ID known to the Directory Server.

OK. Click this button to submit your entry and dismiss the window and return to the Administrator form.

Cancel. Click this button to dismiss the window without submitting your entry information.

Help. Click this button to go to the Online Help window for this topic.

Quota Tab

You use the form accessed through the Message Store Quota tab to define default user disk quotas for the message store. For more information, see also:

- Configuring User Disk Quotas
- Configuring Message Store Partitions

Default user disk quota. This is the amount of storage to be allotted to a user if no disk quota is specified for that user. You can specify either:

- **Unlimited** — Select this option if the default disk quota for users is to be unrestricted.
- **Size specification** — Enter a number in this field to limit user disk quotas. From the pulldown menu, MBytes and KBytes.

Quota warning threshold. In this field, type a number to specify the percentage of disk quota usage which, when exceeded by a user, generates a warning message by the server.

Message to send to the user when quota is exceeded. In this field, enter the contents of the warning message to be sent when a user's disk quota is exceeded.

Over quota grace period. In this field, type a number to indicate how long the messaging server will hold messages in the queue for users who have exceeded their disk quota. From the pulldown menu, choose days or hours.

Save. Click this button to submit and preserve the current disk quota specifications.

Reset. Click this button to return the list contents to the last saved version.

Help. Click this button to go to the Online Help window for this topic.

Partition Tab

You use the form accessed through the Partition tab to view message store partition information, and to add, edit, and delete partition entries. For more information, see also: Configuring Message Store Partitions.

List of partitions. This area lists disk partition information for the message store. This includes the following fields:

- **Default.** This field indicates whether this partition is the default partition for the message store. This is the partition assigned for a user if no partition is specified for that user in the LDAP entry.
- **Nickname.** This field indicates the nickname for the partition. You can use the nickname when configuring user account information.
- **Path.** This field indicates the full physical path for the partition.

Add. Click this button to go to the Add Partition window. This window enables you to add a partition. See Add/Edit Partition Window.

Edit. Click this button to go to the Edit Partition window. This window enables you to edit information about a partition.

Delete. Click this button to delete a partition you've highlighted in the partition list.

Save. Click this button to submit and preserve the current partition list.

Reset. Click this button to return the partition list to the last saved version.

Help. Click this button to get online help for this topic.

Add/Edit Partition Window

The Add Partition and Edit Partition windows are identical. These windows enable you to add or edit a partition entry in the partition list on the Partition form. For more information, see also: Configuring Message Store Partitions

Partition nickname. This is the name you want to assign to the partition.

Partition path. This is the absolute pathname for the specified partition. The partition will be created at this location. The userID used to run the Server must have permission to write to this location, in order to create and manage the partition.

Make this the default partition. Click this box to configure this partition as the default.

OK. Click this button to submit this partition entry and dismiss the window.

Cancel. Click this button to dismiss the window without submitting the partition information.

Help. Click this button to go to the Online Help for this topic.

Aging Tab

The form you access through the Aging tab lists the aging policy for retaining and removing messages from target folders. This form also enables you to define, add, edit, and delete aging rules. For more information, see also: Specifying Aging Policies.

Message store aging rules list. This area lists the aging rules for the message store. The table includes the following fields:

- **Exclusive.** This field indicates whether this rule is the exclusive rule for folders matching a specified pattern.
- **Name.** This field is a name you can assign to the rule for convenience purposes. The name is not used by Messaging Server.
- **Target.** This a pathname, filename, or partial string to be used as the criteria for determining rule targets.
- **Foldersize.** This indicates folder size restrictions to be applied to the target folders. Size can be specified by message count or disk usage (in megabytes or kilobytes). When the folder size is exceeded, the oldest messages are removed until this size is no longer exceeded.
- **Count.** This is the number of messages that will be retained in the target folder(s) before the oldest messages are deleted.
- **Age.** This field indicates the message age constraint for target folders. Messages which have been retained in the target folder(s) longer than the specified number of days are removed.
- **MsgSize.** This field indicates the message size constraint for target folders.
- **Grace Period.** This field indicates how long over-sized messages will remain in the folder before being deleted.

Add. Click this button to go to the Add/Edit Rule window. This window enables you to define an aging rule for the message store.

Edit. Click this button to go to the Add/Edit Rule window. This window enables you to edit a defined aging rule.

Delete. Click this button to delete a rule you've selected in the rules list.

Save. Click this button to submit and preserve the current aging rules list.

Reset. Click this button to return the list contents to the previously saved version.

Help. Click this button to get online help for this topic.

Add/Edit Rule Window

The Add Rule and Edit Rule windows are identical. These windows enable you to define or edit an aging rule entry, and to specify matching patterns for determining rule targets.

Name. Enter the name for the Aging Rule in this field. This is a name you can assign for convenience purposes; it is not used by the Messaging Server.

Apply to folders matching the following pattern. Enter a pathname, filename, or partial string to be used as the criteria for determining rule targets.

Exclusive. Click this selection box to specify that this rule is to be the only rule applied to the target folders.

Message count. In this field, type the maximum number of messages which will be retained in a folder before the oldest messages are removed.

Folder size. In this field, type the maximum size for the target folder. From the pulldown menu, choose `MByte(s)` or `KByte(s)`. When the specified folder size is exceeded, the oldest messages are removed until this size is no longer exceeded.

Number of days. In this field, type the number of days allowed for retaining messages in a target folder. After the specified retention period has elapsed for a given message in a target folder, the message is removed.

Message size limit. In this field, type the maximum allowed size for messages stored in a target folder. From the pulldown menu, choose `MBytes` or `KBytes`.

Grace period. In this field, type a number to indicate the number of days oversized messages are allowed to remain in the folder before being deleted.

OK. Click OK to add the new rule to the rules list and dismiss the window.

Cancel. Click cancel to dismiss the window without submitting the new rule.

Help. Click Help to get online help for this topic.

Chapter

6

Security and Access Control

Netscape Messaging Server supports a full range of flexible security features that allow you to keep messages from being intercepted, prevent intruders from impersonating your users or administrators, and permit only specific people access to specific parts of your messaging system.

The Messaging Server security architecture is part of the security architecture of Netscape servers as a whole. It is built on industry standards and public protocols for maximum interoperability and consistency. To implement Messaging Server security policies, therefore, you will need not only this chapter but several other documents as well. In particular, information in *Managing Servers with Netscape Console* is required for setting up Messaging Server security.

This chapter has the following sections:

- About Server Security
- User Password Login
- Configuring SSL Encryption and Authentication
- Configuring Administrator Access to Messaging Server
- Configuring Client Access to TCP Services
- Interface Reference: Security and Access Control

About Server Security

Server security encompasses a broad set of topics. In most enterprises, ensuring that only authorized people have access to the servers, that passwords or identities are not compromised, that people do not misrepresent themselves as others when communicating, and that communications can be held confidential when necessary are all important requirements for a messaging system.

Perhaps because the security of server communication can be compromised in many ways, there are many approaches to enhancing it. This chapter focuses on setting up encryption, authentication, and access control. It discusses the following security-related Messaging Server topics:

- **User password login:** requiring users to enter passwords to log in to IMAP, POP, or SMTP, and the use of SMTP password login to transmit sender authentication to message recipients
- **SSL encryption and authentication:** setting up your server to use the SSL protocol to encrypt communication and authenticate clients
- **Administrator access control:** using the access-control facilities of Netscape Console to delegate access to a Messaging Server and its individual tasks
- **TCP client access control:** using filtering techniques to control which clients can connect to your server's POP, IMAP, and SMTP services

Not all security and access issues related to Messaging Server are treated in this chapter. Security topics that are discussed elsewhere include the following:

- **Physical security:** Without provisions for keeping server machines physically secure, software security can be meaningless.
- **Program delivery:** Program delivery of messages has significant security implications. See Program Delivery for a discussion.
- **Encrypted messages (S/MIME):** With Secure Multipurpose Internet Mail Extensions, senders can encrypt messages prior to sending them, and recipients can store the encrypted messages after receipt, decrypting them only to read them. Using S/MIME requires no special Messaging Server configuration or tasks; it is strictly a client action. See your client documentation for information on setting it up.

- **Message-store access:** You can define a set of message-store administrators for the Messaging Server. These administrators can view and monitor mailboxes and can control access to them. See Specifying Administrator Access for details.
- **End-user account configuration:** Messaging Server provides limited end-user access (as HTML forms), through which your messaging users can view and change certain information (such as password and vacation message) in their own mail accounts. The end-user forms are described in online help; how to configure the forms is described in Configuring End-User Information.
- **Filtering unsolicited bulk email (UBE):** A Messaging Server plug-in provides flexible filtering options for preventing unwanted commercial email from clogging your users' mailboxes. The UBE plug-in and its use are described in Filtering Unsolicited Bulk Email.

Netscape has produced a large number of documents that cover a variety of security topics. For additional background on the topics mentioned here and for other security-related information, see the Security page on the Netscape DevEdge Web site.

User Password Login

Requiring password submission on the part of users logging into Messaging Server to send or receive mail is a first line of defense against unauthorized access. Messaging Server supports password-based login for its IMAP, POP, and SMTP services.

IMAP and POP Password Login

By default, users must submit a password to retrieve their messages from a Messaging Server. You enable or disable password login for POP separately from IMAP; see Password-Based Login for instructions.

User passwords can be transmitted from the user's client software to your server as clear text or in encrypted form. If either the client or your server are configured to require password encryption, and if both the client and your server support encryption of the required strength (as explained in Enabling SSL), encryption occurs.

User IDs and passwords are stored in your installation's LDAP user directory. Password security criteria, such as minimum length, are determined by directory policy requirements; they are not part of Messaging Server administration.

Certificate-based login is an alternative to password-based login. It is discussed in this chapter along with the rest of SSL; see Setting Up Certificate-Based Login.

SMTP Password Login

By default, users need not submit a password when they connect to the SMTP service of a Messaging Server to send a message. You can, however, require password login to SMTP in order to enable authenticated SMTP.

Authenticated SMTP is an extension to the SMTP protocol, in which message-sender authentication accompanies a message, thus permitting the receiver of the message to know that the sender was authenticated by the sender's mail server. Authenticated SMTP is designed for use within a set of trusted servers in which certificate-based authentication is not being employed. For instructions on enabling SMTP password login (and thus Authenticated SMTP), see Authenticated SMTP.

Figure 6.1 summarizes how Authenticated SMTP works. When SMTP password login is enabled, clients and servers follow this process:

1. When the client connects to its SMTP server to send a message, it first transmits an `auth login` keyword after its `EHLO` command to let the server know that authentication should accompany this message.

   The client typically requires the user to enter a password only once per session, regardless of how many messages the user sends. A client preference allows the user to specify whether to enable or disable authentication.

2. When the sending client's server connects to the next server in the chain of transmission, it performs these two tasks related to client authentication:

   - It authenticates itself to the next server with the `AUTH` command. If the next server supports the `AUTH` command, a password exchange occurs. If the next server does not support `AUTH`, message transmission proceeds but client authentication is dropped.
   - The server passes client authentication on to the next server, using the `AUTH` parameter of the `MAIL FROM` command.

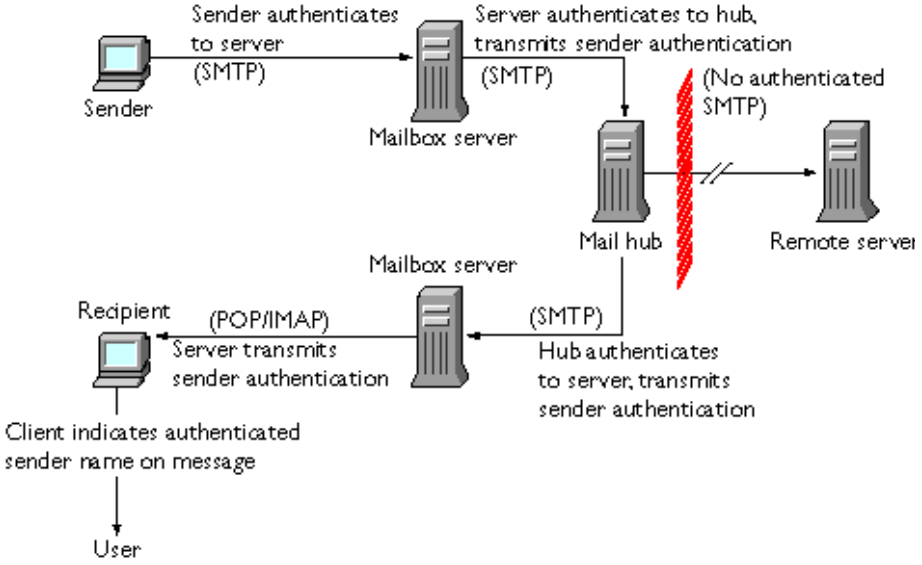
   Note: Because server-password information is stored in an enterprise's LDAP directory, the authentication exchange can occur only between servers that share an LDAP directory--which typically means only servers within a single enterprise. Authenticated SMTP is usually not applied to external message transmission.

3. When the recipient's mail server receives the message, it stores the message in the user's mailbox along with an indication that the sender's name is authenticated.

4. When the user's mail client retrieves the message, it appends an indication of the authentication to the message header. In the Netscape mail client, the word "Internal" appears next to the authenticated sender's name.

You can use Authenticated SMTP with or without SSL encryption.

Figure 6.1 Message transmission with Authenticated SMTP



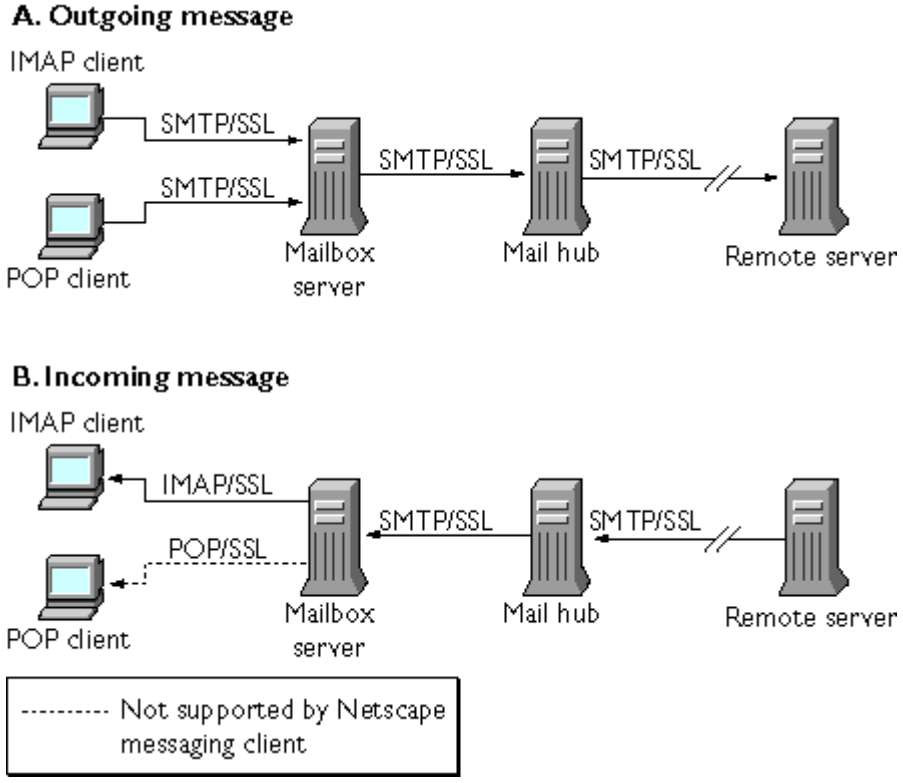
Configuring SSL Encryption and Authentication

Messaging Server uses the Secure Sockets Layer protocol for encrypted communications and for certificate-based authentication of clients and servers. See *Introduction to SSL* (reproduced as an appendix to *Managing Servers with Netscape Console*) for background information on SSL. SSL itself is based on the concepts of public-key cryptography, described in *Introduction to Public-Key Cryptography* (also reproduced as an appendix to *Managing Servers with Netscape Console).*

If transmission of messages between a Messaging Server and its clients and between the server and other servers is encrypted, there is little chance for eavesdropping on the communications. If connecting clients and servers are authenticated, there is little chance for intruders to impersonate (spoof) them.

SSL functions as a protocol layer beneath the application layers of IMAP4, POP3, and SMTP. The SSL version of each of these three application protocols (IMAP/SSL, POP/SSL, SMTP/SSL) acts at a specific stage of message communication, as shown in Figure 6.2 for both outgoing and incoming messages.

Figure 6.2 Encrypted communications with Messaging Server



Complete end-to-end encryption of message transmission may require the use of all three SSL-related protocols. Netscape Messaging Server supports all three, but Netscape's messaging client software supports only SMTP/SSL and IMAP/SSL. As Figure 6.2 shows, the result is that Netscape POP clients can encrypt communication when sending messages, but not when receiving them.

Keep in mind that the extra performance overhead in setting up an SSL connection can put a performance burden on the server. In designing your messaging installation and in analyzing performance, you may need to balance security needs against server capacity.

Netscape Messaging Server 4.0 supports only SSL version 3.0.

> **Note:** Because all Netscape servers support SSL, and the interface for enabling and configuring SSL through Netscape Console is nearly identical across all servers, several of the tasks described in this section are documented more completely in the SSL chapter of *Managing Servers with Netscape Console*. For those tasks, this chapter gives summary information only.

Obtaining Certificates

Whether you use SSL for encryption or for authentication, you need to obtain a server certificate for your Messaging Server. The certificate identifies your server to clients and to other servers.

Managing Internal and External Modules

A server certificate establishes the ownership and validity of a key pair, the numbers used to encrypt and decrypt messages. Your server's certificate and key pair represent your server's identity. They are stored in a certificate database that can be either internal to the server or on an external, removable hardware card (smartcard).

Likewise, the software module that manages the keys and certificates database can be either internal or external. Netscape servers support both internal and external modules that conform to the Public-Key Cryptography System (PKCS) #11 protocol.

Setting up the server for a certificate involves creating a database for the certificate and its keys and installing a PKCS #11 module. If you do not use an external hardware token, you create an internal database on your server, and you use the internal, default module that is part of Messaging Server. If you do use an external token, you connect a hardware smartcard reader and install its PKCS #11 module.

You can manage PKCS #11 modules, whether internal or external, through Netscape Console. To install a PKCS #11 module, you

- connect a hardware card reader to the Messaging Server host machine and install drivers

- use the PKCS #11 Management interface in Netscape Console to connect the PKCS #11 module to the installed driver

(For more complete instructions, see the chapter on SSL in *Managing Servers with Netscape Console*.)

Installing Hardware Encryption Accelerators. If you use SSL for encryption, you may be able to improve server performance in encrypting and decrypting messages by installing a hardware encryption accelerator. An encryption accelerator typically consists of a hardware board, installed permanently in your server machine, plus a software driver. Netscape Messaging Server supports accelerator modules that follow the PKCS #11 protocol. (They are essentially hardware tokens that do not store their own keys; they use the internal database for that.) You install an accelerator by first installing the hardware and drivers as specified by the manufacturer, and then completing the installation--as with hardware certificate tokens--by installing the PKCS #11 module.

Requesting a Server Certificate

You request a server certificate by opening your server in Netscape Console and running the Certificate Setup Wizard, accessed through the Console menu. Using the Wizard, you

- generate a certificate request
- send the request by email to the certificate authority (CA) that is to issue the certificate

When the email response from the CA arrives, you save it as a text file.

(For more complete instructions, see the chapter on SSL in *Managing Servers with Netscape Console*.)

Creating a Password File

On any Netscape server, when you use the Certificate Setup Wizard to request a certificate, the wizard creates a key pair to be stored in either the internal module's database or in an external database (on a smartcard). The wizard then prompts you for a password, which it uses to encrypt the stored key pair. Only that same password can later be used to decrypt the keys. The wizard does not retain the password nor store it anywhere.

On most Netscape servers for which SSL is enabled, the administrator is prompted at startup to supply the password required to decrypt the key pair. On Messaging Server 4.0, however, to alleviate the inconvenience of having to enter the password multiple times (it is need by at least three server processes), and to facilitate unattended server restarts, the password is read from a password file.

The password file must be named `sslpassword.conf` and must be in the directory *`installDirectory`*`/config/`. Entries in the file are individual lines with the format

`moduleName``:`*`password`*

where *`moduleName`* is the name of the (internal or external) PKCS #11 module to be used, and *`password`* is the password that decrypts that module's key pair. The password is stored as clear (unencrypted) text.

Messaging Server 4.0 provides a default version of the password file, with the following single entry (for the internal module and default password):

```
Communicator Certificate DB:netscape!
```

If you specify anything but the default password when you install an internal certificate, you need to edit the above line of the password file to reflect the password you specified. If you install an external module, you need to add a new line to the file, containing the module name and the password you specified for it.

> **Important:** Because the administrator is not prompted for the module password at server startup, it is especially important that you ensure proper administrator access control to the server and proper physical security of the server host machine and server backups.

Installing the Certificate

Installing is a separate process from requesting. Once the email response to your request for a certificate has arrived and been saved as a text file, run the Certificate Setup Wizard once more to install the file as a certificate. When you run the wizard, you

- specify that you are installing a certificate that you have already obtained
- paste the text of your certificate into a field when prompted to do so

(For more complete instructions, see the chapter on SSL in *Managing Servers with Netscape Console*.)

> **Note:** This is also the process you follow to install a CA certificate (described next), which your server uses to determine whether to trust the certificates presented by clients.

Installing Certificates of Trusted CAs

You also use the Certificate Setup Wizard to install the certificates of certificate authorities. A CA certificate validates the identity of the CA itself. Your server uses these CA certificates in the process of authenticating clients and other servers.

If, for example, you set up your enterprise for certificate-based client authentication in addition to password-based authentication (see Setting Up Certificate-Based Login), you need to install the CA certificates of all CAs that are trusted to issue the certificates that your clients may present. These CAs may be internal to your organization or they may be external, representing commercial or governmental authorities or other enterprises. (See *Introduction to Cryptography* for more details on the use of CA certificates for authentication.)

When installed, Messaging Server initially contains CA certificates for several commercial CAs. If you need to add other commercial CAs or if your enterprise is developing its own CA for internal use (using Netscape Certificate Server), you need to obtain and install additional CA certificates.

> **Note:** The CA certificates automatically provided with Messaging Server are not initially marked as trusted. You need to edit the trust settings before your server can trust client certificates issued by these CAs. See Managing Certificates and Trusted CAs for instructions.

To request and install a new CA certificate, you

- contact the certificate authority (possibly through the Web or by email) and request a CA certificate
- save the received the text of the certificate as a text file
- Use the Certificate Setup Wizard, as described in the previous section, to install the certificate.

(For more complete instructions, see the chapter on SSL in *Managing Servers with Netscape Console*.)

Managing Certificates and Trusted CAs

Your server can have more than one server certificate with which it identifies itself. It can also have any number of certificates of trusted CAs that it uses for authentication of clients.

You can view, edit the trust settings of, or delete any of the certificates installed in your Messaging Server by opening your server in Netscape Console and choosing the Certificate Management Command in the Console menu. For instructions, see the chapter on SSL in *Managing Servers with Netscape Console*.

Enabling SSL

You can use Netscape Console to enable SSL and to select the set of encryption ciphers that Messaging Server can use in its encrypted communications with clients.

About Ciphers

A *cipher* is the algorithm used to encrypt and decrypt data in the encryption process. Some ciphers are stronger than others, meaning that a message they have scrambled is more difficult for an unauthorized person to unscramble.

A cipher operates on data by applying a key--a long number--to the data. Generally, the longer the key the cipher uses during encryption, the harder it is to decrypt the data without the proper decryption key.

When a client initiates an SSL connection with a Messaging Server, the client lets the server know what ciphers and key lengths it prefers to use for encryption. In any encrypted communication, both parties must use the same ciphers. Because there are a number of cipher-and-key combinations in common use, a server should be flexible in its support for encryption. Netscape Messaging Server 4.0 can support up to 6 combinations of cipher and key length.

Table 6.1 lists the ciphers that Messaging Server supports for use with SSL 3.0. The table summarizes information that is available in more detail in *Introduction to SSL*; please consult that document before making final decisions on what ciphers to support
.

Table 6.1 SSL ciphers for Messaging Server

Cipher	Description
RC4 with 128-bit encryption and MD5 message authentication	The fastest encryption cipher (by RSA) and a very high-strength combination of cipher and encryption key. Suitable only for domestic North American (non-export) use.
Triple DES with 168-bit encryption and SHA message authentication	A slower encryption cipher (a U.S. government-standard) but the highest-strength combination of cipher and encryption key. Suitable only for domestic North American (non-export) use.
DES with 56-bit encryption and SHA message authentication	A slower encryption cipher (a U.S. government-standard) and a moderate-strength combination of cipher and encryption key. Suitable only for domestic North American (non-export) use.
RC4 with 40-bit encryption and MD5 message authentication	The fastest encryption cipher (by RSA) and a lower-strength combination of cipher and encryption key. Suitable for international use.
RC2 with 40-bit encryption and MD5 message authentication	A slower encryption cipher (by RSA) and a lower-strength combination of cipher and encryption key. Suitable for international use.
No encryption, only MD5 message authentication	No encryption; use of a message digest for authentication alone.

Unless you have a compelling reason for not using a specific cipher, you should support them all. However, note that export laws restrict the use of certain encryption ciphers in certain countries. Basically, key lengths of greater than 40 bits can be used only in the United States and Canada. See *Export Restrictions on International Sales* on the Netscape DevEdge Web site for details. In general, Messaging Server cannot use the higher-strength encryption for any communication with international versions of client software.

Turning On SSL and Selecting Ciphers

If your Messaging Server has an installed server certificate, SSL is enabled as long as one or more encryption ciphers is selected. (Most are on by default.) Thus you can effectively enable or disable SSL communications by selecting or deselecting encryption ciphers. Follow these steps:

1. In Netscape Console, open the Messaging Server whose cipher settings you want to modify.
2. Click the Configuration tab in the left pane.
3. Select the Services folder.
4. Select the Encryption tab in the right pane. The Encryption Configuration form opens.
5. Click the boxes to select the encryption cipher or ciphers that you want your server to support. To disable SSL completely, deselect all ciphers.

See Encryption Configuration Tab for a complete description of the contents of that form.

Setting Up Certificate-Based Login

In addition to password-based authentication, Netscape servers support authentication of users through examination of their digital certificates. In certificate-based authentication, the client establishes an SSL session with the server and submits the user's certificate to the server. The server then evaluates whether the submitted certificate is genuine. If the certificate is validated, the user is considered authenticated.

To set up your Messaging Server for certificate-based login:

1. Obtain a server certificate for your server. (See Obtaining Certificates for details.)
2. Run the Certificate Setup Wizard to install the certificates of any trusted certificate authorities that will issue certificates to the users your server will authenticate. (See Installing Certificates of Trusted CAs for details.)

Note that, as long as there is at least one trusted CA in the server's database, the server requests a client certificate from each connecting client.

3. Turn on SSL. (See Enabling SSL for details.)

4. (Optional) Edit your server's `certmap.conf` file so that the server appropriately searches the LDAP user directory based on information in the submitted certificates.

   Editing the `certmap.conf` file is not necessary if the email address in your users' certificates matches the email address in your users' directory entries, and if you do not need to optimize searches or validate the submitted certificate against a certificate in the user entry.

   For details of the format of `certmap.conf` and the changes you can make, see the SSL chapter of *Managing Servers with Netscape Console*.

Once you have taken these steps, when a client establishes an SSL session so that the user can log in to IMAP, the Messaging Server requests the user's certificate from the client. If the certificate submitted by the client has been issued by a CA that the server has established as trusted, and if the identity in the certificate matches an entry in the user directory, the user is authenticated and access is granted (depending on access-control rules governing that user).

There is no need to disallow password-based login (see Password-Based Login) to enable certificate-based login. If password-based login is allowed (which is the default state), and if you have performed the tasks described in this section, both password-based and certificate-based login are supported. In that case, if the client establishes an SSL session and supplies a certificate, certificate-based login is used. If the client does not use SSL or does not supply a certificate, the server requests a password.

For more details on setting up your entire installation of Netscape servers and clients to use certificate-based authentication, see *Single Sign-On Deployment Guide*.

Configuring Administrator Access to Messaging Server

This section describes how to control the ways in which server administrators can gain access to Messaging Server. Administrative access to a given Messaging Server and to specific Messaging Server tasks occurs within the context of delegated administration. *Delegated administration* is a feature of all Netscape servers; it refers to the capability of an administrator to provide other administrators with selective access to individual servers and server features. For an overview of delegated administration, see the chapter on delegating server administration in *Managing Servers with Netscape Console*.

> **Note:** Most tasks described in this section are common to all Netscape servers, and are therefore described fully only in the chapter on delegating server administration in *Managing Servers with Netscape Console*. This chapter briefly summarizes the tasks.

Hierarchy of Delegated Administration

When you install the first Netscape server on your network, the installation program automatically creates a group in the LDAP user directory called the Configuration Administrators group. By default, the members of the Configuration Administrators group have unrestricted access to all hosts and servers on your network.

The Configuration Administrators group is at the top of an access hierarchy, such as the following, that you can create to implement delegated administration for Messaging Server:

1. **Configuration administrator.** The "super user" for the network of Netscape servers. Has complete access to all resources.

2. **Domain administrator.** The configuration administrator typically creates one or more other groups, each with more restricted access. For example the configuration administrator might create a Domain Administrators group and give it access to all server for a specific administrative domain in the network. (An *administrative domain* is the set of hosts and servers on the network that share the same user directory for looking up account information.)

3. **Server administrator.** A domain administrator might create groups to administer each type of server. For example, a Messaging Administrators group might be created to administer all Messaging Servers in an administrative domain or across the whole network. Members of that group have access to all Messaging Servers (but no other servers) in that administrative domain.

4. **Task administrator.** Finally, any of the above administrators might create a group, or designate an individual user, with restricted access to a single Messaging Server or a set of Messaging Servers. Such a task administrator is permitted to perform only specific, limited server tasks (such as starting or stopping the server only, or accessing logs of a given service).

Netscape Console provides convenient interfaces that allow an administrator to

- grant a group or an individual access to a specific Messaging Server, as described in Providing Access to the Server as a Whole (next)
- restrict that access to specific tasks on a specific Messaging Server, as described in Restricting Access to Specific Tasks

Providing Access to the Server as a Whole

To give a user or group permission to access a given instance of Messaging Server, you

- log in to Netscape Console as an administrator with access to the Messaging Server you want to provide access to
- select that server in the Console window, and choose Set Access Permissions in the Console menu
- add or edit the list of users and groups with access to the server

(For more complete instructions, see the chapter on delegating server administration in *Managing Servers with Netscape Console*):

Once you have set up the list of individuals and groups that have access to the particular Messaging Server, you can then use ACIs, as described next, to delegate specific server tasks to specific people or groups on that list.

Restricting Access to Specific Tasks

An administrator typically connects to a server to perform one or more administrative tasks. Common administrative tasks are listed in the Messaging Server Tasks form in Netscape Console (see Figure 1.12).

By default, access to a particular Messaging Server means access to all of its tasks. However, each task in the Task form can have an attached set of access-control instructions (ACIs). The server consults those ACIs before giving a connected user (who must already be a user with access permissions to the server as a whole) access to any of the tasks. In fact, the server displays in the Tasks form only those tasks to which the user has permission.

If you have access to a Messaging Server, you can create or edit ACIs on any of the tasks (that is, on any of the tasks to which you have access), and thus restrict the access that other users or groups can have to them.

To restrict the task access that a connected user or group can have, you

- log in to the Netscape Console as an administrator with access to the Messaging Server you want to provide restricted access to
- open the server and select a task in the server's Tasks form
- choose Set Access Permissions from the Edit menu, and add or edit the list of access rules to give a user or group the kind of access you want them to have.
- Repeat the process for other tasks, as appropriate

(For more complete instructions, see the chapter on delegating server administration in *Managing Servers with Netscape Console*):

For example, suppose you want to create a group of administrators responsible for log analysis, and you also have an individual (Miranda) who is responsible for filtering out unsolicited bulk email (UBE). You can

1. create a group called Logging Admins and add the appropriate people to it
2. use Set Access Permissions for the Netscape Console Configuration window to give both Logging Admins and Miranda access to the Messaging Server

3. use Set Access Permissions for the Messaging Server Tasks form to place ACIs on the various tasks, making sure that the Logging Admin group sees (and thus has access to) only the logging-related tasks, and that Miranda sees only the UBE filter-configuration task

ACIs and how to create them are described more fully in the chapter on delegating server administration in *Managing Servers with Netscape Console*.

Configuring Client Access to TCP Services

Messaging Server supports sophisticated access control on a service-by-service basis for its TCP-based services (IMAP, POP, and SMTP), so that you can exercise far-ranging and fine-grained control over which users can gain access to your server.

If you are managing messaging services for a large enterprise or an Internet service provider, these capabilities can help you to exclude spammers and DNS spoofers from your system and improve the general security of your network. For control of spam mail (unsolicited bulk email) specifically, see also Chapter 8, Filtering Unsolicited Bulk Email.

> **Note:** If controlling user access is *not* an important issue for your enterprise, you do not have to create any of the filters described in this section. If minimal access control is all you need, see the section Mostly Allowing for instructions on setting it up.

How Client Access Filters Work

The Messaging Server access-control facility for TCP clients is an implementation of the TCP wrapper concept. A *TCP wrapper* is a program that listens at the same port as the TCP daemon it serves; it uses access filters to verify client identity, and it gives the client access to the daemon if the client passes the filtering process. The design of the Messaging Server TCP wrapper is based on the Unix `Tcpd` access-control facility (created by Wietse Venema) and the `identd` service (described in Internet draft RFC 1413).

As part of its processing, the Messaging Server TCP client access-control system performs (when necessary) the following analyses of the socket end-point addresses:

- Reverse DNS lookups of both end points (to perform name-based access control)
- Forward DNS lookups of both end points (to fight DNS spoofing)
- `Identd` callback (to check that the user on the client end is known to the client host)

The system compares this information against access-control statements called *filters* to decide whether to grant or deny access. For each service, separate sets of Allow filters and Deny filters control access. Allow filters explicitly grant access; Deny filters explicitly forbid access.

When a client requests access to a service, the access-control system compares the client's address or name information to each of that service's filters--in order--using these criteria:

- The search stops at the first match. Because Allow filters are processed before Deny filters, Allow filters take precedence.
- Access is granted if the client information matches an Allow filter for that service.
- Access is denied if the client information matches a Deny filter for that service.
- If no match with any Allow or Deny filter occurs, access is granted--except in the case where there are Allow filters but no Deny filters, in which case lack of a match means that access is denied.

The filter syntax described here is flexible enough that you should be able to implement many different kinds of access-control policies in a simple and straightforward manner. You can use both Allow filters and Deny filters in any combination, even though you can probably implement most policies by using almost exclusively Allows or almost exclusively Denies.

The following sections describe filter syntax in detail and give usage examples.The section Creating Access Filters with Netscape Console gives the procedure for creating access filters.

Filter Syntax

Filter statements contain both server information and client information. The server information can include the name of the service, names of hosts, and addresses of hosts. The client information can include host names, host addresses, and user names. Both the server and client information can include wildcard names or patterns.

The very simplest form of a filter is

service: hostSpec

where *service* is the name of the service (such as `smtp`, `pop`, or `imap`) and *hostSpec* is the host name, IP address, or wildcard name or pattern that represents the client requesting access. When a filter is processed, if the client seeking access matches *hostSpec*, access is either allowed or denied (depending on which type of filter this is) to the service specified by *service*. Here are two examples:

```
imap: roberts.newyork.airius.com

pop: ALL
```

If these are Allow filters, the first one grants the host `roberts.newyork.airius.com` access to the IMAP service, and the second one grants all clients access to the POP service. If they are Deny filters, they deny those clients access to those services. (See Wildcard Names for descriptions of wildcard names such as `ALL`.)

Either the server or the client information in a filter can be somewhat more complex than this, in which case the filter has the more general form of

serviceSpec: clientSpec

where *serviceSpec* can be either *service* or *service@hostSpec*, and *clientSpec* can be either *hostSpec* or *user@hostSpec*. *user* is the user name (or a wildcard name) associated with the client host seeking access. Here are two examples:

```
smtp@mailServer1.airius.com: ALL

imap: srashad@xyz.europe.airius.com
```

If these are Deny filters, the first filter denies all clients access to the SMTP service on the host `mailServer1.airius.com`. The second filter denies the user `srashad` at the host `xyz.europe.airius.com` access to the IMAP

service. (See Server-Host Specification and Client User-Name Specification for more information on when to use these expanded server and client specifications.)

Finally, at its most general, a filter has the form

serviceList: *clientList*

where *serviceList* consists of one or more *serviceSpec* entries, and *clientList* consists of one or more *clientSpec* entries. Individual entries within *serviceList* and *clientList* are separated by blanks and/or commas.

In this case, when a filter is processed, if the client seeking access matches any of the *clientSpec* entries in *clientList*, then access is either allowed or denied (depending on which type of filter this is) to all the services specified in *serviceList*. Here is an example:

```
pop, imap: .europe.airius.com .newyork.airius.com
```

If this is an Allow filter, it grants access to both POP and IMAP services to all clients in either of the domains `europe.airius.com` and `newyork.airius.com`. (See Wildcard Patterns for information on using a leading dot or other pattern to specify domains or subnets.)

Wildcard Names

You can use the following wildcard names to represent service names, host names or addresses, or user names:

Wildcard Name	Explanation
ALL	The universal wildcard. Matches all names.
LOCAL	Matches any local host (one whose name does not contain a dot character). However, if your installation uses only canonical names, even local host names will contain dots and thus will not match this wildcard.

Wildcard Name	Explanation
UNKNOWN	Matches any user whose name is unknown, or any host whose name or address is unknown. Use this wildcard name carefully: • Host names may be unavailable due to temporary DNS server problems--in which case all filters that use UNKNOWN will match all client hosts. • A network address is unavailable when the software cannot identify the type of network it is communicating with--in which case all filters that use UNKNOWN will match all client hosts on that network.
KNOWN	Matches any user whose name is known, or any host whose name *and* address are known. Use this wildcard name carefully: • Host names may be unavailable due to temporary DNS server problems--in which case all filters that use KNOWN will fail for all client hosts. • A network address is unavailable when the software cannot identify the type of network it is communicating with--in which case all filters that use KNOWN will fail for all client hosts on that network.
DNSSPOOFER	Matches any host whose DNS name does not match its own IP address.

Wildcard Patterns

You can use the following patterns in server or client addresses:

- A string that begins with a dot character (`.`). A host name is matched if the last components of its name match the specified pattern. For example, the wildcard pattern `.airius.com` matches all hosts in the domain `airius.com`.

- A string that ends with a dot character (`.`). A host address is matched if its first numeric fields match the specified pattern. For example, the wildcard pattern `123.45.` matches the address of any host in the subnet `123.45.0.0`.
- A string of the form `n.n.n.n/m.m.m.m`. This wildcard pattern is interpreted as a *`net/mask`* pair. A host address is matched if *`net`* is equal to the bitwise AND of the address and *`mask`*. For example, the pattern `123.45.67.0/255.255.255.128` matches every address in the range `123.45.67.0` through `123.45.67.127`.

EXCEPT Operator

The access-control system supports a single operator. You can use the `EXCEPT` operator to create exceptions to matching names or patterns when you have multiple entries in either *`serviceList`* or *`clientList`*. For example, the expression

`list1` `EXCEPT` *`list2`*

means that anything that matches *`list1`* is matched, *unless* it also matches *`list2`*.

Here is an example:

```
ALL: ALL EXCEPT isserver.airius.com
```

If this were a Deny filter, it would deny access to all services to all clients except those on the host machine `isserver.airius.com`.

`EXCEPT` clauses can be nested. The expression

`list1` `EXCEPT` *`list2`* `EXCEPT` *`list3`*

is evaluated as if it were

`list1` `EXCEPT (` *`list2`* `EXCEPT` *`list3`*`)`

Server-Host Specification

You can further identify the specific service being requested in a filter by including server host name or address information in the *`serviceSpec`* entry. In that case the entry has the form

`service@hostSpec`

You may want to use this feature when your Messaging Server host machine is set up for multiple internet addresses with different internet host names. If you are a service provider, you can use this facility to host multiple domains, with different access-control rules, on a single server instance.

Client User-Name Specification

For client host machines that support the `identd` service as described in RFC 1413, you can further identify the specific client requesting service by including the client's user name in the *`clientSpec`* entry in a filter. In that case the entry has the form

`user@hostSpec`

where *`user`* is the user name as returned by the client's `identd` service (or a wildcard name).

Specifying client user names in a filter can be useful, but keep these caveats in mind:

- The `identd` service is not authentication; the client user name it returns cannot be trusted if the client system has been compromised. In general, do not use specific user names; use only the wildcard names `ALL`, `KNOWN`, or `UNKNOWN`.
- User-name lookups take time; performing lookups on all users may slow access by clients that do not support `identd`. Selective user-name lookups can alleviate this problem. For example, a rule like

  `serviceList``: @xyzcorp.com ALL@ALL`

  would match users in the domain `xyzcorp.com` without doing user-name lookups, but it would perform user-name lookups with all other systems.

The user-name lookup capability can in some cases help you guard against attack from unauthorized users on the client's host. It is possible in some TCP/IP implementations, for example, for intruders to use `rsh` (remote shell service) to impersonate trusted client hosts. If the client host supports the `ident` service, you can use user-name lookups to detect such attacks. See Allowing Only Identified Users for an example and discussion.

Filter Examples

The examples in this section show a variety of approaches to controlling access. In studying the examples, keep in mind that Allow filters are processed before Deny filters, the search terminates when a match is found, and access is granted when no match is found at all.

The examples listed here use host and domain names rather than IP addresses. Remember that you can include address and netmask information in filters, which can improve reliability in the case of name-service failure.

Mostly Denying

In this case, access is denied by default. Only explicitly authorized hosts are permitted access.

The default policy (no access) is implemented with a single, trivial deny file:

```
ALL: ALL
```

This filter denies all service to all clients that have not been explicitly granted access by an Allow filter. The Allow filters, then, might be something like these:

```
ALL: LOCAL @netgroup1
ALL: .acme.com EXCEPT externalserver.acme.com
```

The first rule permits access from all hosts in the local domain (that is, all hosts with no dot in their host name) and from members of the group `netgroup1`. The second rule uses a leading-dot wildcard pattern to permit access from all hosts in the `acme.com` domain, with the exception of the host `externalserver.acme.com`.

Mostly Allowing

In this case, access is granted by default. Only explicitly specified hosts are denied access.

The default policy (access granted) makes Allow filters unnecessary. The unwanted clients are listed explicitly in Deny filters such as these:

```
ALL: externalserver.acme.com, .airius.asia.com
ALL EXCEPT pop: contractor.acme.com, .airius.com
```

The first filter denies all services to a particular host and to a specific domain. The second filter permits nothing but POP access from a particular host and from a specific domain.

Allowing Only Identified Users

You can use the following Deny filter to exclude all users but those known to a client host's `identd` service:

```
ALL: UNKWOWN@ALL
```

The filter denies all services to all unknown users from all domains.

You could write a more specific Deny filter, with a *`clientSpec`* entry of `UNKNOWN@`*`host`*. When it receives a request from *`host`*, the access-control system then uses the `ident` service on *`host`* to find out whether that host actually sent the request and what the user name of the requestor is. If the host responds that the sending user is unknown, that may be evidence of an attack. (However, note also that, if the client's host does not support the `identd` service, all requestors will match the `UNKNOWN@`*`host`* filter.)

Employing user-name lookups in Allow filters is less trustworthy. Suppose you write an Allow filter with a *`clientSpec`* entry of `KNOWN@`*`host`*. Because an intruder can spoof both the client connection and the `ident` lookup, a match with the `KNOWN@`*`host`* filter is not strong evidence of absence of spoofing. Furthermore, if the client system has been compromised (as noted earlier), `ident` may return false information.

See Client User-Name Specification for more information.

Denying Access to Spoofed Domains

You can use the `DNSSPOOFER` wildcard name in a filter to detect host-name spoofing. When you specify `DNSSPOOFER`, the access-control system performs forward or reverse DNS lookup to verify that the client's presented host name matches its actual IP address. Here is an example for a Deny filter:

```
ALL: DNSSPOOFER
```

This filter denies all services to all remote hosts whose IP addresses don't match their DNS host names.

Controlling Access to Virtual Domains

If your messaging installation uses virtual domains, in which a single server instance is associated with multiple IP addresses and domain names, you can control access to each virtual domain through a combination of Allow and Deny filters. For example, you can use Allow filters like

```
ALL@msgServer.domain1.com: @.domain1.com

ALL@msgServer.domain2.com: @.domain2.com

...
```

coupled with a Deny filter like

```
ALL: ALL
```

Each Allow filter permits only hosts within `domain`*`N`* to connect to the service whose IP address corresponds to `msgServer.domain`*`N`*`.com`. All other connections are denied.

Denying an Individual User

If you must deny access to an especially notorious individual user, the most general Deny filter you can apply is the following:

```
ALL: badUser@ALL
```

This filter cannot, of course, guard against the same person attempting to gain access under a different user name.

Creating Access Filters with Netscape Console

You create and edit Allow and Deny filters through a separate Netscape Console separately for each service. Follow these steps to create filters:

1. In Netscape Console, open the Messaging Server that you want to create access filters for.

1. Click the Configuration tab.

2. Open the Services folder in the left pane and select IMAP, POP, or SMTP beneath the Services folder.

3. Click the Access tab in the right pane.

   The Access form is displayed. The Allow and Deny fields in the form show the existing Allow and Deny filters for that service. Each line in the field represents one filter. For either of the fields, you can any of the following actions:

   - Click Add to create a new filter. An Allow Filter window or Deny filter window opens; enter the text of the new filter into the window, and click OK.

   - Select a filter and click Edit to modify the filter. An Allow Filter window or Deny filter window opens; edit the text of the filter displayed in the window, and click OK.

     (See IMAP Allow Filter Window, IMAP Deny Filter Window, POP Allow Filter Window, POP Deny Filter Window, SMTP Allow Filter Window, and SMTP Deny Filter Window for complete descriptions of the contents of those windows.)

   - Select a filter and click Delete to remove the filter.

   Note: If you need to rearrange the order of Allow or Deny filters, you can do so by performing a series of Delete and Add actions.

See IMAP Access Tab, POP Access Tab, and SMTP Access Tab for complete descriptions of the contents of those forms.

For a specification of filter syntax and a variety of examples, see the next section, Filter Syntax. For additional examples, see Filter Examples.

Interface Reference: Security and Access Control

This section describes the Netscape Console interface elements that allow you to configure security settings and access control for Messaging Server. See *Managing Servers with Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

Encryption Configuration Tab

You use the form accessed through this tab to enable SSL and to select the encryption ciphers that your Messaging Server uses for communication with clients.

For more information, see also Enabling SSL.

The Encryption Configuration form has the following elements:

Cipher Settings. Click one or more of these checkboxes to permit the use of the specified encryption ciphers. Click a previously checked box to disable the specified cipher. See About Ciphers for more information about these ciphers.

SSL is enabled if one or more of these ciphers is checked and your server has an installed server certificate.

> **Note:** Export versions of Netscape Messaging Server may not support all ciphers available on Domestic U.S. versions.

Action Buttons

Save. Click this button to save any settings you have made in the Encryption Configuration form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the Encryption Configuration form.

IMAP Access Tab

You use the form accessed through this tab to control user access to the IMAP service.

For more information, see also

- Configuring Client Access to TCP Services
- Creating Access Filters with Netscape Console

The IMAP Access form has the following elements:

Allow Filters

Allow. This field displays Allow filters--access-control rules that permit access to the IMAP service. Any IMAP client that matches any of the Allow filters in this field is allowed IMAP access. You can edit the contents of this field by clicking the Add button, or by selecting a line in this field and then clicking Edit or Delete.

Add. Click this button to open a window (see IMAP Allow Filter Window) that allows you to add a new Allow filter to the Allow field.

Edit. Click this button to open a window (see IMAP Allow Filter Window) that allows you to edit the Allow filter that is currently highlighted in the Allow field.

Delete. Click this button to delete the Allow filter that is currently highlighted in the Allow field.

Deny Filters

Deny. This field displays Deny filters--access-control rules that deny access to the IMAP service. Any IMAP client that matches any of the Deny filters in this field is denied IMAP access. You can edit the contents of this field by clicking the Add button, or by selecting a line in this field and then clicking either Edit or Delete.

Add. Click this button to open a window (see IMAP Deny Filter Window) that allows you to add a new Deny filter to the Deny field.

Edit. Click this button to open a window (see IMAP Deny Filter Window) that allows you to edit the Deny filter that is currently highlighted in the Deny field.

Delete. Click this button to delete the Deny filter that is currently highlighted in the Deny field.

Action Buttons

Save. Click this button to save any settings you have made in the IMAP Access form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the IMAP Access form.

IMAP Allow Filter Window

You use this window to add or edit Allow filters, the rules by which clients are permitted to access the IMAP service.

For more information, see also

- Creating Access Filters with Netscape Console
- “Filter Syntax” on page 194

The IMAP Allow Filter window has the following elements:

ALLOW filter. Use this field to enter a new IMAP Allow filter or edit the one currently being displayed. A typical Allow filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be accessed (`imap` in this case), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be allowed access to the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of IMAP Allow filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the ALLOW filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of IMAP Allow filters unchanged.

Help. Click this button to display online help (this document) that describes the IMAP Allow Filter window.

IMAP Deny Filter Window

You use this window to add or edit Deny filters, the rules by which clients are explicitly excluded from access to the IMAP service.

For more information, see also

- Creating Access Filters with Netscape Console
- Filter Syntax

The IMAP Deny Filter window has the following elements:

DENY filter. Use this field to enter a new IMAP Deny filter or edit the one currently being displayed. A typical Deny filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be denied (imap in this case), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be prevented from accessing the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of IMAP Deny filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the DENY filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of IMAP Deny filters unchanged.

Help. Click this button to display online help (this document) that describes the IMAP Deny Filter window.

POP Access Tab

You use the form accessed through this tab to control user access to the POP service.

For more information, see also

- Configuring Client Access to TCP Services
- Creating Access Filters with Netscape Console

The POP Access form has the following elements:

Allow Filters

Allow. This field displays Allow filters--access-control rules that permit access to the POP service. Any POP client that matches any of the Allow filters in this field is allowed POP access. You can edit the contents of this field by clicking the Add button, or by selecting a line in this field and then clicking either Edit or Delete.

Add. Click this button to open a window (see POP Allow Filter Window) that allows you to add a new Allow filter to the Allow field.

Edit. Click this button to open a window (see POP Allow Filter Window) that allows you to edit the Allow filter that is currently highlighted in the Allow field.

Delete. Click this button to delete the Allow filter that is currently highlighted in the Allow field.

Deny Filters

Deny. This field displays Deny filters--access-control rules that deny access to the POP service. Any POP client that matches any of the Deny filters in this field is denied POP access. You can edit the contents of this field by clicking the Add button, or by selecting a line in this field and then clicking either Edit or Delete.

Add. Click this button to open a window (see POP Deny Filter Window) that allows you to add a new Deny filter to the Deny field.

Edit. Click this button to open a window (see POP Deny Filter Window) that allows you to edit the Deny filter that is currently highlighted in the Deny field.

Delete. Click this button to delete the Deny filter that is currently highlighted in the Deny field.

Action Buttons

Save. Click this button to save any settings you have made in the POP Access form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the POP Access form.

POP Allow Filter Window

You use this window to add or edit Allow filters, the rules by which clients are permitted to access the POP service.

For more information, see also

- Creating Access Filters with Netscape Console
- Filter Syntax

The POP Allow Filter window has the following elements:

ALLOW filter. Use this field to enter a new POP Allow filter or edit the one currently being displayed. A typical Allow filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be accessed (in this case, pop), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be allowed access to the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of POP Allow filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the ALLOW filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of POP Allow filters unchanged.

Help. Click this button to display online help (this document) that describes the POP Allow Filter window.

POP Deny Filter Window

You use this window to add or edit Deny filters, the rules by which clients are explicitly excluded from access to the POP service.

For more information, see also

- Creating Access Filters with Netscape Console
- Filter Syntax

The POP Deny Filter window has the following elements:

DENY filter. Use this field to enter a new POP Deny filter or edit the one currently being displayed. A typical Deny filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be denied (in this case, pop), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be prevented from accessing the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of POP Deny filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the DENY filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of POP Deny filters unchanged.

Help. Click this button to display online help (this document) that describes the POP Deny Filter window.

SMTP Access Tab

You use the form accessed through this tab to control client access to the SMTP service.

For more information, see also:

- Configuring Client Access to TCP Services
- Creating Access Filters with Netscape Console

The SMTP Access form has the following elements:

Allow Filters

Allow. This field displays Allow filters--access control rules that permit access to the SMTP service. Any SMTP client that matches any of the Allow filters in this field is allowed SMTP access. You can edit the contents of this field by selecting a line in this field and then clicking one of the following three buttons.

Add. Click this button to open a window (see SMTP Allow Filter Window) that allows you to add a new Allow filter to the Allow field.

Edit. Click this button to open a window (see SMTP Allow Filter Window) that allows you to edit the Allow filter that is currently highlighted in the Allow field.

Delete. Click this button to delete the Allow filter that is currently highlighted in the Allow field.

Deny Filters

Deny. This field displays Deny filters--access control rules that deny access to the SMTP service. Any SMTP client that matches any of the Deny filters in this field is denied SMTP access. You can edit the contents of this field by selecting a line in this field and then clicking one of the following three buttons.

Add. Click this button to open a window (see SMTP Deny Filter Window) that allows you to add a new Deny filter to the Deny field.

Edit. Click this button to open a window (see SMTP Deny Filter Window) that allows you to edit the Deny filter that is currently highlighted in the Deny field.

Delete. Click this button to delete the Deny filter that is currently highlighted in the Deny field.

Action Buttons

Save. Click this button to save any settings you have made in the SMTP Access form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns to the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) that describes the SMTP Access form.

SMTP Allow Filter Window

You use the SMTP Allow Filter window to add or edit Allow filters, the rules by which clients are permitted to access the SMTP service.

For more information, see also

- Creating Access Filters with Netscape Console
- Filter Syntax

The SMTP Allow Filter window has the following elements:

Allow filter. Use this field to enter a new SMTP Allow filter or edit the one currently being displayed. A typical Allow filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be accessed (`smtp` in this case), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be allowed access to the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of SMTP Allow filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the ALLOW filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of SMTP Allow filters unchanged.

Help. Click this button to display online help (this document) that describes the SMTP Allow Filter window.

SMTP Deny Filter Window

You use the SMTP Deny Filter window to add or edit Deny filters, the rules by which clients are explicitly excluded from access to the SMTP service.

For more information, see also

- Creating Access Filters with Netscape Console
- Filter Syntax

The SMTP Deny Filter window has the following elements:

Deny filter. Use this field to enter a new SMTP Deny filter or edit the one currently being displayed. A typical Deny filter has the format

serviceSpec:*clientSpec*

where *serviceSpec* is generally the name of the service to be accessed (smtp in this case), and *clientSpec* is typically a host name, domain name, or wildcard name or pattern. Clients that match the information in *clientSpec* are to be allowed access to the service specified in *serviceSpec*.

For a complete syntax description, see Filter Syntax.

Examples. This non-editable field displays examples of SMTP Deny filters. For additional examples, see Filter Examples.

Action Buttons

OK. Click this button to save the entry or the edits you have made in the DENY filter field.

Cancel. Click this button to cancel the entry or edit, leaving the set of SMTP Deny filters unchanged.

Help. Click this button to display online help (this document) that describes the SMTP Deny Filter window.

Chapter

7

Working With SMTP Plug-Ins

This chapter describes how to install and configure SMTP plug-ins, dynamic libraries that extend the capabilities of Messaging Server. For instructions on how to develop SMTP plug-ins, and for a detailed description of the plug-in programming interface, see *Messaging Server Plug-In API Guide*.

For information on using the specific SMTP plug-in that allows you to filter unsolicited bulk email (UBE), see Chapter 8, Filtering Unsolicited Bulk Email.

This chapter contains the following sections:

- About SMTP Plug-Ins
- Managing SMTP Plug-Ins with Netscape Console
- Interface Reference: SMTP Plug-Ins

About SMTP Plug-Ins

Netscape Messaging Server 4.0 provides an application programming interface (API) that allows third parties to create server plug-ins that can add site-specific functionality to Messaging Server. Developers use the Messaging Server Plug-in API to

- process the message header and body at specific times, before the message undergoes further processing by Messaging Server

- split the message among envelope recipients and change the envelope sender

Message-processing plugins can include character-set converters or content filters that implement site-specific firewall functionality, filtering out suspicious incoming or outgoing attachments. Message-splitting plug-ins can be used to customize the message content for a subset of the original recipients.

Messaging Server SMTP plug-ins act at two stages in message processing:

- post-`SMTPAccept` (immediately after the message is received)
- pre-`SMTPDeliver` (just before the message is handed off to another host).

Messaging Server 4.0 includes one pre-built plug-in, the UBE plugin (see Chapter 8, Filtering Unsolicited Bulk Email). It provides a flexible, customizable filtering capability for removing or redirecting unwanted messages.

For more information about server plug-in APIs, see *Messaging Server Plug-In API Guide*. For general Netscape developer information, see the Netscape DevEdge site.

Managing SMTP Plug-Ins with Netscape Console

The SMTP plug-ins that you can use with Netscape Messaging Server may include

- the Netscape UBE plug-in
- plug-ins that your enterprise has developed internally
- commercially developed plug-ins that you have purchased

See your Netscape sales or support representative for information about the availability of plug-ins for Messaging Server 4.0.

As administrator, you control which plug-ins are installed and active at any given time. Plug-ins may have very different purposes, but they are all installed and activated in the same way.

Installing Plug-Ins

Only one plug-in (the UBE plug-in) is installed automatically when you install Messaging Server. Other plug-ins come with documentation describing how to install and configure them.

Follow these steps to install a plug-in:

1. Copy the plug-in library file to a suitable location on your server host machine.
2. In Netscape Console, open the Messaging Server on that host machine.
3. Click the Configuration tab and open the Services folder in the left pane.
4. Open the SMTP icon under the Services folder, and select Plugins under the SMTP icon. The SMTP Plugins form appears in the right pane.

   (See SMTP Plugins Tab for a complete description of the contents of that form.)
5. Click Add to open the Add Plugin window.
6. In the Add Plugin window, specify the following information for your new plug-in:

   - In the entry field, select the entry point in SMTP processing at which your plug-in operates (`postSmtpAccept` or `preSmtpDeliver`).
   - In the Path field, enter the pathname to the plug-in library file.
   - In the Functions field, enter a comma-separated list of the names of the functions that this plug-in provides. Your plug-in documentation should state exactly what to enter in this field.
   - Options: any other required information (in the form of comma-separated *`name=value`* pairs) as specified in the documentation accompanying the plug-in.
7. Click OK to commit your entries and install the plug-in.
8. Restart the server.

See Add/Edit Plugin Window for a complete description of the contents of the Add Plugin window.

> **Note:** Your plug-in may have additional installation procedures not described here. See the documentation accompanying the plug-in for more information.

By default, a newly installed plug-in is not active. To activate your new plug-in, see Activating and Deactivating Plug-Ins.

The information you enter in the Add Plugin window is written to your Messaging Server's `plugins.cfg` file. See Manually Installing and Configuring Plug-Ins for information on installing plug-ins by directly editing `plugins.cfg`.

Deleting (Uninstalling) Plug-Ins

Follow these steps to remove an installed plug-in from your Messaging Server, using Netscape Console:

1. Open the SMTP Plugins form, as described in Installing Plug-Ins.
2. In the Plugin Configuration table, select the pathname of the plug-in you want to delete.
3. Click Delete.

   > **Note:** This uninstallation removes the plug-in library file and makes corresponding modifications to the configuration file `plugins.cfg`. If your plug-in includes other files, you may have additional uninstallation steps to follow. See the documentation accompanying your plug-in for more information.

You can also remove a plug-in by editing and deleting files manually. See Manually Installing and Configuring Plug-Ins for instructions.

Activating and Deactivating Plug-Ins

All installed plug-ins appear in the Messaging Server SMTP Plugins form in Netscape Console. Follow these steps to activate or deactivate a plug-in:

1. Open the SMTP Plugins form, as described in Installing Plug-Ins.
2. In the Plugin Configuration table, locate the pathname of the plug-in you want to activate or deactivate.
3. Check the Status box to the left of the plug-in's pathname to activate the plug-in; uncheck the Status box to deactivate the plug-in.
4. Click OK.

   Note: If the plug-in you want to activate or deactivate does not appear in the table, it may not be installed or it may have been installed improperly. If it was installed improperly, remove it by following the instructions in Manually Deleting Plug-Ins, and then try again.

The active or inactive status of a plug-in is stored in the `plugins.cfg` file. See Manually Installing and Configuring Plug-Ins for information on activating and deactivating plug-ins by directly editing `plugins.cfg`.

Configuring Plug-Ins

You initially configure a plug-in when you first install it (see Installing Plug-Ins). You can also use Netscape Console to change the configuration of an installed plug-in.

Follow these steps to reconfigure an installed plug-in:

1. Open the SMTP Plugins form, as described in Installing Plug-Ins.
2. In the Plugin Configuration table, select the pathname of the plug-in you want to reconfigure.
3. Click Edit. The Edit Plugin window opens.
4. In the Edit Plugin window, modify any of the following information as needed:

- In the Entry field, change the entry point in SMTP processing at which this plug-in operates (`postSmtpAccept` or `preSmtpDeliver`).
- In the Path field, edit the pathname to the plug-in library.
- In the Functions field, edit the comma-separated list of the functions that this plug-in provides.
- In the Options field, edit any other required information, as specified in the documentation accompanying the plug-in.

5. Click OK to commit your reconfiguration of the plug-in.

See Add/Edit Plugin Window for complete documentation of the contents of the Edit Plugin window.

The information you enter in the Edit Plugin window is written to your Messaging Server `plugins.cfg` file. See Manually Installing and Configuring Plug-Ins for information on reconfiguring plug-ins by directly editing `plugins.cfg`.

> **Note:** Your plug-in may have additional configuration files and procedures not described here. See the documentation accompanying the plug-in for more information.

Managing SMTP Plug-Ins Manually

You are not required to use Netscape Console to manage your SMTP plugins. This section describes how to manage them by editing the plug-in configuration file.

Manually Installing and Configuring Plug-Ins

You can install and configure an SMTP plug-in by directly editing your Messaging Server `plugins.cfg` file. That file is located at *`instanceDirectory`*`/smtp-bin/plugins/`, where *`instanceDirectory`* is the directory containing the files of the specific instance of the Messaging Server that uses the plug-in.

The `plugins.cfg` file holds basic configuration information for all installed plug-ins. In the configuration file, plug-ins are listed in the order in which you installed them in the Messaging Server. When they run, the plug-ins for a given entry point are also executed in that order. If order of execution is important, either make sure you install plug-ins in the order you want, or edit `plugins.cfg` to achieve that order.

Each plug-in's configuration is a line with these elements:

`entry pluginPath` `funcs=`*`functionList`* `[`*`optionList`*`]`

where the elements have the following meanings:

`entry`	The entry point (`PostSmtpAccept` or `PreSmtpDeliver`) at which this plug-in operates.
`pluginPath`	The pathname to the plug-in library's binary (executable) file.
`functionList`	A comma-separated list of the functions supported by this plug-in. Messaging Server calls these functions, in the order in which they appear in this list, to execute the plug-in.
`optionList`	An optional set of comma-separated *`name=value`* pairs that the plug-in can use for any purpose. Messaging Server passes this information to the plug-in when it executes the plug-in.

Here is a example for a Unix server with a (fictional) character-set translator plug-in:

```
PostSmtpAccept /usr/local/lib/char_xlate.so
funcs=xlate_charset
no_xlate_domain = *.fr
```

This plug-in acts at `PostSmtpAccept`, its library name is `char_xlate.so`, it has a single function (`xlate_charset`), and it uses a single option that tells it not to translate messages from the top-level domain `.fr`.

Here is an example for a Windows NT server with the UBE filter plug-in:

```
PostSmtpAccept i:\Netscape\Server4\msg-Airius1\
   smtp-bin\libUBEfilter.dll
funcs=filter_msg_plugin config=i:\Netscape\
   Server4\msg-Airius1\smtp-bin\plugins\UBEfilter.opt
option=i:\Netscape\Server4\msg-Airius1\smtp-bin\plugins\UBEfilter.opt
```

This plug-in also acts at `PostSmtpAccept`, its library name is `libUBEFilter.dll`, it has a single function (`filter_msg_plugin`), and it uses two options (named `config` and `option`) that specify pathnames to configuration files.

You can modify the information in any of these lines to change the configuration of the plug-in. For example, if you change the location of the plug-in library file, you can enter the new path here instead of using the Netscape Console interface. (This would be equivalent to reinstalling the plug-in, and would require a server restart.)

If a plug-in is installed but has been deactivated through Netscape Console, its line in the `plugins.cfg` file is commented out; that is, it starts with a number sign (#) character. You also can manually deactivate a plug-in by commenting out its lines in the file.

> **Note:** If your plug-in uses other files besides its library file and `plugins.cfg`, configuring the plug-in may mean editing those files as well. For details, see the documentation that accompanies your plug-in.

Manually Deleting Plug-Ins

To manually delete, or uninstall, a plug-in, take these steps:

1. Deactivate the plug-in if it is active.
2. Delete the plug-in's lines from `plugins.cfg`
3. Remove the plug-in library file from your server host machine.

4. Remove any other plug-in-specific configuration files, as noted in the documentation that accompanies the plug-in.

Interface Reference: SMTP Plug-Ins

This section describes the Netscape Console interface elements that allow you to install and configure SMTP plug-ins. See *Managing Servers With Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

SMTP Plugins Tab

You use the form accessed through this tab to install and remove SMTP plug-ins. For more information, see also

- Installing Plug-Ins
- Deleting (Uninstalling) Plug-Ins
- Activating and Deactivating Plug-Ins
- Configuring Plug-Ins

The SMTP Plugins form has these elements:

Plugin Configuration. This table displays the status and location of each installed plug-in. Use the Path entry to select a plug-in; then use the Add, Edit, and Delete buttons to add it, delete it, or change its configuration.

> **Note:** If you have installed a plug-in but it does not appear in this field, it may not have been installed properly. In that case, remove it by following the instructions in Manually Deleting Plug-Ins, and then try again.

Status. Check this box to make an installed plug-in active; uncheck the box to make an installed plug-in inactive.

Path. This entry within the Plugin Configuration table displays the path to (location of) each installed plug-in. To edit this entry, select it and click Edit.

Add. Click this button to open the Add Plugin window (see Add/Edit Plugin Window), which allows you to install a new SMTP plug-in.

Edit. After selecting a plug-in in the Plugin Configuration table, click this button to open the Add Plugin window (see Add/Edit Plugin Window), which allows you to edit the configuration of the selected plug-in.

Delete. After selecting a plug-in in the Plugin Configuration table, click this button to remove the selected plug-in.

Action Buttons

Save. Click this button to commit any settings you have made in the SMTP Plugins form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns the settings it had when you last clicked Save).

Help. Click this button to get online help (this document) describing the SMTP Plugins form.

Add/Edit Plugin Window

You use this window to install a new SMTP plug-in or edit the characteristics of a currently installed plug-in. For more information, see also

- Installing Plug-Ins
- Configuring Plug-Ins
- *Messaging Server Plug-In API Guide* (for information on plug-in structure)

The Add/Edit Plugin window has these elements:

Entry. Use this list to select the entry point (`PostSmtpAccept` or `PreSmtpDeliver`) for this plug-in.

Path. Use this field to enter the location of (path to) the plug-in library itself. You must have already placed your plug-in library in its location before entering this information.

Functions. Use this field to enter the list of functions that this plug-in implements. The list is a comma-separated sequence of function names. The documentation accompanying the plug-in you are installing or reconfiguring should provide this information.

Options. Use this field to enter additional information (in the form of comma-separated *name=value* pairs) that is to be passed to the plug-in when it is executed. The documentation accompanying the plug-in you are installing or reconfiguring should provide this information.

Action Buttons

OK. Click this button to commit the information you have entered, installing the new plug-in or imposing the changes you have made to the existing one.

Cancel. .Click this button to close the Edit Plugin window without making any additions or changes to the current set of plug-ins.

Help. Click this button to display online help (this document) that describes the Edit Plugin window.

Chapter

8

Filtering Unsolicited Bulk Email

This chapter describes the unsolicited bulk email (UBE) plug-in and the filters it uses to help you screen out unsolicited email. For information on Messaging Server plug-ins in general, see Chapter 7, Working With SMTP Plug-Ins.

This chapter contains the following sections:

- About the UBE Plug-In
- UBE Filter Format
- Managing UBE Filters With Netscape Console
- Creating Filters Manually
- Extending the UBE Plug-In
- Interface Reference: UBE Filters

About the UBE Plug-In

The UBE plug-in is an SMTP plug-in that works as an extension to Netscape Messaging Server. You can use it to design and implement filters that can block unsolicited bulk email from reaching your users.

What Is UBE?

Unsolicited bulk mail is email sent to large numbers of recipients without their knowledge or consent, often advertising commercial products or services. It is the electronic equivalent of paper junk mail. For a full definition, see the Web-based document *Unsolicited Bulk Email: Definitions and Problems*.

Users of email services are sometimes inundated with unsolicited bulk mail and may expect their service providers to address the problem. One approach that providers can follow is to use filters that selectively eliminate email whose characteristics mark it as UBE. Netscape Messaging Server provides both a plug-in architecture and a scriptable plug-in module that can be used to cut down on (though probably never completely eliminate) UBE.

UBE Filters and the UBE Plug-In

The UBE plug-in is an SMTP plug-in to Netscape Messaging Server. SMTP plug-ins are dynamically loaded software modules that access the Messaging Server Plug-in API, an application programming interface. The plug-ins function by intercepting incoming and outgoing messages, analyzing them for certain characteristics, and taking appropriate action before possibly passing them on. SMTP Plug-ins are described in general in Chapter 7, Working With SMTP Plug-Ins.

The UBE plug-in is provided as part of Messaging Server 4.0. It is a customizable plug-in that works by examining all incoming mail before it is routed throughout the system (to users' mailboxes or to other email servers). The UBE plug-in uses a set of rules (called *filters*), contained in a configuration file, to decide how to handle each piece of mail. Any mail not affected by any of the filters continues on its normal course, untouched by the plug-in.

The UBE plug-in supports a simple scripting language that is useful for processing and directing the flow of messages. You use the language to create the filters that intercept and block or otherwise handle UBE messages. You can use the Netscape Console interface to create and edit filters, or you can perform those tasks manually by editing the UBE configuration file directly.

How UBE Filters Work

A UBE filter is a line in a text file (default name = `UBEfilter.cfg`). When you create a filter, you define a criterion to which email messages are compared. Whenever an email message meets the criterion defined in the filter definition, the filter triggers the action that you designated in the filter definition.

For example, if you don't want to get any messages from `uglymail.com`, you can create a UBE filter that identifies any email message from `uglymail.com`. You can then designate `REJECT` as the action to be performed by the UBE plug-in.

In using the UBE plug-in, you can create many different types of UBE filters and activate or deactivate them individually. You can manipulate your set of UBE filters through the Netscape Console interface, or through direct editing of the configuration file in which they are stored. This chapter describes both methods.

UBE Filter Format

A UBE filter is a single text line containing 3 to 5 parts, in this order:

`[:`*`label`*`]` *`messageField matchCriterion action`* `[`*`argument`*`]`

Here is an example filter that includes all five parts:

```
:DontSend Subject "Bad mail" REJECT "Do not send mail"
```

The following subsections use this example to describe, in order, the parts that make up a filter.

Label

The label is an identifying name for the filter. This part is optional and is used only if this filter is the destination of another filter's `JUMP` action. (See Table 8.1 for a description of the `JUMP` action.)

The label is always preceded by a colon (`:`).

Example: `:DontSend`

Message Field

The message field is the portion of the message header or envelope that the filter analyzes. Each arriving message has header fields that hold information about that message. The filter can use any of the fields in deciding how to handle the mail. There is no complete list of possible header fields since the format is open (see Internet Draft RFC 822 for a list of the defined standard fields), but common fields include `To`, `From`, `Sender`, `Reply-To`, `Content-type`, and so on. See Table 8.3 for descriptions of some of the most common fields.

Example: `Subject`

After the message field name you can place a colon (`:`) followed by special tags that affect how the message field is processed. Currently, two special tags are supported: `case` and `envonly`.

case Tag

The `case` tag causes the matching criterion (which follows the message field in the filter) to be treated as case sensitive. By default, filters are not case sensitive. Here's an example of two filters, identical except for the `case` tag:

```
Subject:case "Bad mail" REJECT "Do not send mail"

Subject "Bad mail" REJECT "Do not send mail"
```

The first filter would intercept only those messages whose subject is `Bad mail`; the second filter would intercept messages whose subject is either `Bad mail` or `bad mail` (or even `bAd mAiL`).

envonly Tag

The `envonly` tag instructs the filter to consider only envelope information, rather than all message-header information, for the message field. Because header information is more easily altered by a mail sender than is envelope information, you can use this tag to help resist spoofing attacks based on header information.

For example, `Auth-Sender` is an envelope field, added by a server sending a message by authenticated SMTP, that identifies the sender of the message.You might design a filter that examines that field to ensure that only authenticated mail gets through. A tricky user could, however, add a phony `Auth-Sender` field to the header information in a message, possibly defeating your filter. If you restrict the message field to `envonly`, only those fields that are created by the server, and thus are harder to tamper with, will be considered.

> **Note:** Using the `envonly` tag makes sense only if your UBE plug-in has been configured to include header fields by default; see Envelope Fields and Header Fields for an explanation.

Match Criterion

The match criterion is the string (or regular expression) that the filter looks for in the contents of the message field to see whether a match is achieved. The combination of message field and match criterion is called the filter's *predicate;* the state of the predicate (matched or unmatched) determines whether or not the filter is to be applied.

Predicate example: `Subject "Bad mail"`

In this example, if the Subject field of the message being analyzed is `Bad mail`, the filter is applied; otherwise, the filter is not applied. Note that, in the absence of a `case` tag, the match criterion is not case sensitive.

The match criterion is a regular expression, so you can use it to match a wide variety of strings. For example, to match any Subject field containing the phrase "Get Rich Quick", you can specify `".*Get Rich Quick.*"` as the match criterion. See Regular Expressions for Match Criterion for more information.

Action

The action field defines the action that the UBE plug-in performs if a match occurs. As soon as a match occurs with any filter predicate, the action associated with that filter is taken. Filter processing stops when a *terminal action* (one that stops processing) is taken, or when the end of the filter file is reached. See Table 8.1 for descriptions of the actions.

Example: `REJECT`

This action causes the message to be returned to the sender.

You can also apply the negation modifier to reverse the conditions under which an action occurs; see Negation Modifier.

Argument

The argument field contains any additional information that may be needed to perform the specified action. Some actions do not take an argument, whereas others do. See Table 8.1 for descriptions of the arguments used by each of the actions.

Example: `"Do not send mail"`

In this case, `"Do not send mail"` is the argument to the `REJECT` action; it is a message that accompanies the returned mail.

Available Actions for UBE Filters

Table 8.1 lists the actions that you can specify in a UBE filter. Each action is classified either as terminal (filter processing stops as soon as it is taken) or non-terminal (processing continues after it is taken).

Table 8.1 UBE filter actions

Action	Argument	Description
`COPY`	Comma-separated list of addresses	Adds these recipients to the original set of recipients, then continues processing the next filter. (Non-terminal action.)
	Example: `Channel-To "user1@domain1\.com" COPY "postmaster, user2"` In this case, any mail sent to `user1@domain1.com` is also sent to `postmaster` and to `user2`.	

Table 8.1 UBE filter actions (Continued)

Action	Argument	Description
`DROP`	One address	Replaces original set of recipients with this one and sends the message on. (Terminal action.)
	Example: `User-From ".*@bulk\.com" DROP "postmaster"` In this case, any mail from any account at `bulk.com` is sent to `postmaster` but no one else.	
`EXIT`	(none)	Immediately stops filter processing and sends the message on. Subsequent filters in the configuration file are not applied to this message. (Terminal action.)
	Example: `User-From "CEO@.*" EXIT` In this case, any mail from a user named `CEO` is sent through.	
`HOLDCOPY`	Comma-separated list of addresses, followed by a vertical bar (`|`) and a message string	Holds the message. Sends a notification--containing the original message and the message string in the argument--to the recipients listed in the argument. (Terminal action.)
	Example: `Subject "Free stuff!" HOLDCOPY "postmaster | please handle"` In this case, any mail containing the subject `"Free stuff!"` is held, with a copy sent to `postmaster`.	

Table 8.1 UBE filter actions (Continued)

Action	Argument	Description
HOLDONLY	Comma-separated list of addresses, followed by vertical bar (|) and a message string	(Same as HOLDCOPY, except that it does not copy the original message.) Sends a notification containing the message string in the argument--but without including the original message--to the recipients listed in the argument. (Terminal action.)
	Example: `Subject "Free stuff!" HOLDCOPY "postmaster | please handle"` In this case, any mail containing the subject `"Free stuff!"` is held, with a notification sent to `postmaster`.	
JUMP	Label (filter name)	Shifts filter processing to the named filter, skipping any intervening filters. The named filter must exist in the configuration file. (Non-terminal action.)

	Example:
	`Subject "Easy $$$" JUMP "MoneyReject"`
	`subject".*$$$.*" HOLDCOPY "postmaster | evaluate for $$$"`
	`:MoneyReject Subject "Easy $$$" REJECT "No commercials, please"`
	
	In this case, mail with the specific subject `"Easy $$$"` is rejected, whereas other mail with triple dollar signs in the subject is held for the postmaster to evaluate.	

REJECT	Reject reason (message string)	Returns the mail to the sender and includes the reject reason in the message. (Terminal action.)
	Example: `User-from "Pitchman@cheapstuff\.com" REJECT "Do not advertise to our users"` In this case, any mail from `Pitchman@cheapstuff.com` is automatically returned along with the message `"Do not advertise to our users"`.	

Table 8.1 UBE filter actions (Continued)

Action	Argument	Description
RUN	Command line to execute	Executes the specified program, passing the message header and body to the program. The program must be located in the directory *INSTANCEDIR*/smtp-bin/plugins where *INSTANCEDIR* is the instance directory (name = msg-*instancename*). You can use the special field name $& in the subsequent filter to match the return value of the program. (Non-terminal action.)
	Example: `Subject "May contain a virus" RUN "VirusScan.exe" $& "1" REJECT "Message rejected due to presence of virus!"` In this case, any mail with the subject "May contain a virus" is sent to the program VirusScan.exe for analysis. If the return value from the program is 1, the message is returned along with the message "Message rejected due to presence of virus!".	

Regular Expressions for Match Criterion

The UBE filter supports extended regular expressions compliant with POSIX 1003.2. There are many sources of information on regular expressions; this document is not intended as a reference.

Table 8.2 lists some of the common regular-expression special characters and constructions that you can use in creating match criteria for UBE filters.

Table 8.2 Regular-expression special characters

Characters	Usage
`.`	(Dot). Matches any single character.
`[]`	(Brackets). Matches any single character from the set of characters specified within the brackets. The brackets may enclose the entire set of permissible characters (`[2468]`), or they may specify an ASCII range, using end points and a hyphen (`[a-z]`). For example, `r[eo]d` matches `red` and `rod`, but not `rid` or `reed`. `x[0-9]` matches `x0`, `x1`, `x2`, and so on, but not `x11`.
`[^]`	(Caret in brackets). Matches any single character that is *not* one of those specified within the brackets following the caret. (The caret must be the first character in the brackets.) For example, `r[^eo]d` matches `rid` but not `red` or `rod`. `x[^0-9]` matches `xa`, `xb`, `xc`, and so on, but not `x2`.
`*`	(Asterisk). Matches zero or more of the immediately preceding character or expression. For example, `ba*c` matches `bc`, `bac`, `baac`, and so on. The expression `.*` matches any string.
`+`	(Plus) Matches one or more of the immediately preceding character or expression. For example, `ba+c` matches `bac`, `baac`, and so on. `r[eo]+d` matches `red`, `rod`, `reed` and `rood`, but not `reod` or `roed`.
`\`	(Backslash) The Escape character. It removes the pattern-matching significance of the character it precedes, so that special characters (like those in this table) can be matched as regular ASCII characters. For example, `.` matches any character, but `\.` matches only the dot character. (To match the backslash character itself, you must precede it with another backslash: `\\`.)
`\~`	(Escaped tilde) Matches any character but the subsequent character. For example, `b\~ad` matches `bbd`, `bcd`, `b3d`, but not `bad`.

Table 8.2 Regular-expression special characters (Continued)

Characters	Usage
`\{\}`	(Escaped braces) Matches any number of occurrences of the exact sequence of characters between the escaped braces. For example, `\{ju\}+fruit` matches `jufruit`, `jujufruit`, `jujujufruit`, and so on. It does not match `jfruit`, `ufruit`, or `ujfruit`. You can use the expression `\{ \}` to match any number of spaces between words.
`\{`*x*`\!`*x*`\}`	(Escaped bang in escaped braces) Matches any one of the characters *x* separated by the alternation symbol (`\!`). For example, `\{j\!u\}+fruit` matches `jfruit`, `jjfruit`, `ufruit`, `ujfruit`, `uufruit`, `uuufruit`, and so on.
^	(Caret) Matches the beginning of a line.
$	(Dollar sign) Matches the end of a line.
`()`	(Parentheses) Delimits arguments. You can explicitly limit the extent of a regular expression by enclosing it in parentheses. For example, `uuufruit` is a single regular expression, but you can force it to be considered two separate expressions by applying parentheses, as in `(uuu)(fruit)`. For an example of the use of parentheses, see the example filter following Table 8.4.

Many other rules define, for example, what a character is and how characters in regular expressions may be juxtaposed for various purposes. Please consult any POSIX 1003.2-compliant regular-expression documentation for more information.

Envelope Fields and Header Fields

Every message has two types of fields that you can include in the message-field part of your filters. Header fields are created by a mail client when it sends a message. Envelope fields are created by mail servers that send or resend the message during its transit from sender to receiver. By default, the UBE plug-in examines envelope fields only. This restriction exists for performance reasons, because the header can contain any number of fields.

The envelope fields most useful for filter purposes include those listed in Table 8.3.

Table 8.3 Common envelope fields for UBE filters

Envelope field	Description
`Submitted-Date`	The date on which the server received the message.
`Host-From`	The IP address of the machine that directly connected to and transferred the message to this Messaging Server. You can use this field to, for example, separate external mail from mail of local origin.
`User-From`	The value of the SMTP `mail-from` command. The value in this field is not validated unless you have enabled the "Verify each recipient's address when accepting messages" setting. (See Verifying Recipient Addresses for instructions.) You can use this field to, for example, ensure that you accept (or perhaps reject) messages only from specific known users.
`Auth-Sender`	If authenticated SMTP is being used for this message, this field contains the email address of the authenticated user that sent the message. (Note that this field contains the email address of the user, not the user name or password used to authenticate the user.) You can use this field to, for example, accept mail only from authenticated users.
`MAIL-Exts`	A list of any extensions to SMTP (such as delivery notification) that were passed to the SMTP daemon through the `mail-from` SMTP command. Extensions are listed exactly as entered in the command.
`Channel-To`	The list of recipients for this message, as listed in the `rcpt-to` SMTP command. Each recipient is listed on a separate line, with this format: `<user@xyzcorp.com>`
`RCPT-Exts`	A list of any extensions to SMTP (such as delivery notification) that were passed to the SMTP daemon through the `rcpt-to` SMTP command. Extensions are listed exactly as entered in the command.

Table 8.3 Common envelope fields for UBE filters

Envelope field	Description
`Message-Size`	The total size, in bytes, of the header plus body of the received message. You can use the value in this field to, for example, drop messages that are too large.
`MTA-Hops`	The number of SMTP servers (not including this one) that the received message has passed through. You can use the value in this field to, for example, drop messages that have been relayed through too many machines.

If you want to include header fields as well as envelope fields in your filter predicates, you can use the Netscape Console interface (see Unsolicited Bulk Email Configuration Tab). You can also accomplish this manually, by adding the following line to your filter options file (`UBEfilter.opt`):

```
parseheader: 1
```

This instruction tells the UBE plug-in to look at both envelope and header fields when comparing a message to a filter.

If you have set the default to include header fields, you can then, on a filter-by-filter basis, force the plug-in to look only at the envelope fields by using the `envonly` flag in the message field of your filter; see envonly Tag for a description of the flag.

> **Note:** If you are designing your filters to operate on header fields as well as envelope fields, you can use your mail client to help decide which header fields to analyze. With the Netscape Messenger mail client in Netscape Communicator, you can view the complete set of header fields in a received message by choosing All from the Headers menu (accessed from the View menu).

Special Message-Field Names

You can use special field names to combine filters and narrow your criteria. Table 8.4 describes these names, using the following filter as an example:

```
Subject "This is ."   REJECT "This is bad mail"
```

(Note that this example includes a dot wildcard, which matches any single character, in the match criterion.)

Table 8.4 Special message-field names for UBE filters

Special name	Explanation
`$0`	Represents the complete message field content that was last matched. Assume that the message just compared against the above example filter had the subject "This is a test". Then the current value of `$0` would be `"This is a test"`.
`$1`	Represents the exact matching portion of the message field content that was last compared. In the above example, again assuming that the message subject was "This is a test", the value of `$1` after the comparison would be `"This is a"`. An example of the use of `$1` follows this table.
`$2..$9`	Represent the values, in order, of any parenthetical matches you may have specified in your match criterion. If, in the above example, your match criterion had been `"(This) (is) (a) (test)"`, and again assuming that the message subject was "This is a test", the comparison would yield the results `$2=this`, `$3=is`, `$4=a`, and `$5=test`.
`$&`	Represents the numerical result code of the last action. You can use this special field name in conjunction with the `RUN` action (see Table 8.1).

Table 8.4 Special message-field names for UBE filters (Continued)

Special name	Explanation
$#	Represents the number of recipients in the current message. A comparison of this value and a number is considered true if this value is equal to or greater than the given number. You can use this field name to, for example, block all messages with more than a maximum permitted number of recipients.

$ANY	Represents any field. Using this special name causes the plug-in to compare your match criterion with all fields. For example, you can use it to search all header fields for a specific phrase, as in this predicate:
	
	`$ANY "get free stuff"`
	
	You can also use it to match all messages, with a predicate such as
	
	`$ANY ".*"`
	
	which will match any field containing any string.

The following example uses both a special field name and parenthesized expression parsing:

```
:handleFrom   User-From   (.*)@airius.com   !JUMP   handleregular
              $1          "postmaster"       JUMP   handleAIRIUSpost
              ""          ""                 JUMP   handleregular
```

- The first line (labeled `:handleFrom`) looks at the senders of the message, using parentheses (as described in Table 8.2) to match against the user name. Only if the mail is from someone at Airius corporation does execution continue to the next line. (See the next section for an explanation of the exclamation point modifier.)
- The second line states that, if the message is exactly from the `postmaster` account at Airius, execution should jump to the filter line that handles Airius postmaster messages.

- The third line causes processing of other messages to jump to another location. The message field and match criterion are not needed for this filter, so they are replaced by empty quotes; see Omitting Parts of a Filter for an explanation.

Negation Modifier

You can modify an action by applying the negation operator to it. Normally, the action specified in a filter is taken if the match criterion is matched. If, however, the negation operator is applied to the action, the action is *not* taken if the criterion is matched; conversely, the action *is* taken if the criterion is *not* matched.

For example, the following filter accepts all messages originating from within Airius Corporation:

```
Sender ".*airius\.com" EXIT
```

A complementary filter might reject all messages that are not local:

```
Sender ".*airius\.com" !REJECT "local mail only"
```

If you are using the Netscape Console interface to create filters, you click a button to apply the negation modifier; if you are creating filters manually, you apply the modifier as a prefix to the action, as shown in the example.

Managing UBE Filters With Netscape Console

The UBE plug-in is installed automatically when you install Messaging Server 4.0; see *Installing Messaging Server 4.0* for more information. This section explains how to use Netscape Console to activate the UBE plugin and to create, edit, activate, and change the order of individual filters.

Details of filter format and instructions for designing filters using Netscape Console are given in UBE Filter Format. Note that you can also create and manipulate filters manually; see Creating Filters Manually for details.

Activating the UBE Plug-In

To make the UBE plug-in available for use, use Netscape Console to access the SMTP Plugins form (see Activating and Deactivating Plug-Ins). Turn on the UBE plug-in in the Plugin Configuration table. (Its name is `libUBEfilter.so` or `libUBEfilter.sl` for Unix; `libUBEfilter.dll` for Windows NT.)

As with all SMTP plug-ins, basic configuration of the UBE plug-in is controlled by the contents of the configuration file `plugins.cfg`. Individual filter characteristics and other aspects of UBE plug-in execution are controlled by the files `UBEfilter.cfg` and `UBEfilter.opt`. See Plug-In File and Configuration Files for more information.

Creating a New Filter

Follow these steps to create a new UBE filter from Netscape Console:

1. In Netscape Console, open the Messaging Server whose UBE plug-in you want to add a new filter to.

2. Follow either of these steps to access the UBE Configuration form:

   - Click the Tasks tab, then click "Configure Unsolicited Bulk Email Filters".

   - Click the Configuration tab, open the Services folder in the left pane, and open the SMTP icon beneath the Services folder. Open the Plugins icon beneath the SMTP folder icon, and select UBE beneath the Plugins icon. Click the Unsolicited Bulk Email tab in the right pane.

   The UBE Configuration form is displayed.

   (See Unsolicited Bulk Email Configuration Tab for a complete description of the contents of that form.)

3. Click "Add a filter." The "Add a UBE Filter" window opens.

4. (Optional) Assign a label to the new filter. The label is needed only in certain circumstances; see Label.

5. Specify a message field to use for matching. Either select a field from the popup menu in the "If" field or enter the field name directly into the "If" field. The field names in the popup menu correspond to the parts of the header or envelope information attached to an email message. See Message Field.

6. Choose equals (=) or does not equal (!=). If you choose =, the UBE plug-in acts only when a match between a message and this filter occurs. If you choose !=, the plug-in acts only when a match between a message and this filter does *not* occur. See Negation Modifier.

7. Type a value (the match criterion) in the Value field. This is the value (generally a string or regular expression) that the UBE plug-in compares with the contents of the message field you specified above. See Match Criterion.

8. Select an action from the popup menu in the "Then" field. This is the action the UBE plug-in will perform on any email that matches this filter (or does not match, if you chose (!=) in Step 4). See Action.

9. If required by the action you selected, enter an argument for that action in the Argument field. Some actions require arguments, such as addresses to forward mail to. See Argument.

10. When you have finished creating the UBE filter, click OK. The new UBE filter appears in the list of UBE filters in the UBE Configuration form.

11. Back in the UBE Configuration form, click Save to save the new UBE filter.

See Add/Edit UBE Filter Window for a complete description of the contents of the Add UBE Filter window.

IMPORTANT: Newly created filters are not saved until you click Save, even though they may appear in the UBE Configuration form.

Note: New filters are automatically saved as active. If you want to deactivate your new filter, follow the instructions in Activating and Deactivating Filters.

You can also create a new UBE filter by directly editing the filter configuration file. See Creating Filters Manually.

Editing an Existing Filter

Follow these steps to edit an existing UBE filter from Netscape Console:

1. Access the UBE Configuration form, as described in Creating a New Filter.
2. In the Filters field, click to highlight the UBE filter that you want to edit.
3. Click the Edit button. The "Edit a UBE Filter" window opens, displaying the parts of the UBE filter you're editing.
4. Make any desired changes to the filter, specifying the contents of the fields, as described in Creating a New Filter.
5. When you have finished editing the filter, click OK. The revised filter appears in the same place it previously occupied in the UBE configuration form.

   IMPORTANT: When you edit a UBE filter, the edited filter replaces the original one. You cannot create a new filter by editing an existing filter and, for example, saving it with a new name (label). To create a new filter, see Creating a New Filter.
6. Back in the UBE Configuration form, click Save to save the edited filter.

See Add/Edit UBE Filter Window for a complete description of the contents of the Edit UBE Filter window.

IMPORTANT: Changes made to filters are not saved until you click Save, even though they may appear changed in the UBE Configuration form.

You can also modify an existing UBE filter by directly editing the filter configuration file. See Creating Filters Manually.

Activating and Deactivating Filters

Active filters are designated with a check in the Active box next to the filter definition in the UBE Configuration form. You can activate or deactivate filters individually, and you can activate or deactivate all filters at once. Follow these steps:

1. Access the UBE Configuration form, as described in Creating a New Filter.
2. Do any of the following:
   - To activate all filters, click "Activate all filters."
   - To deactivate all filters, click "Deactivate all filters."
   - To activate a single inactive filter, check the Active box next to it.
   - To deactivate a single active filter, uncheck the Active box next to it.
3. When you have finished activating or deactivating filters, click Save.

   IMPORTANT: The changes you make to the active state of filters are not saved until you click Save.

You can also activate and deactivate UBE filters by directly editing the filter configuration file. See Creating Filters Manually.

Changing the Order of Filters

Incoming email messages are compared to UBE filters in the order in which the filters appear in the UBE Configuration form. Depending on how you design your filters, the order in which they are applied to incoming email messages may be important. Follow these steps to change the order of the filters in the UBE Configuration form:

1. Access the UBE Configuration form, as described in Creating a New Filter.
2. Click the up or down arrow next to the filter you want to move. If necessary, continue clicking the appropriate arrow until the filter you are moving is in the desired position relative to the other UBE filters in the list.

3. Repeat step 2 for each filter you want to move.

4. When you have finished changing the order of your UBE filters, click Save.

   IMPORTANT: The changes you make in the order of your UBE filters are not saved until you click Save, even though they may appear reordered in the UBE Configuration form.

You can also reorder UBE filters by directly editing the filter configuration file. See the section Creating Filters Manually.

Parsing Header Fields

You can specify that the UBE plug-in examine header fields as well as envelope fields when applying the filters to a message. (By default, the plug-in looks only at envelope fields.) Follow these steps:

1. Access the UBE Configuration form, as described in Creating a New Filter.

2. Check the "Parse message header" box to specify that the UBE plug-in should parse message headers as well as envelopes. See Envelope Fields and Header Fields for more information.

You can also set this option manually. See Plug-In File and Configuration Files for more information.

Creating Filters Manually

If you are designing a lengthy and complex set of UBE filters, it may be more efficient to create and edit them manually, rather than through the Netscape Console interface. This section describes how to create, delete, modify, activate, and deactivate UBE filters without using Netscape Console. To do this, you must understand the configuration files used by the UBE plug-in and how to edit them.

Plug-In File and Configuration Files

The UBE plug-in is an SMTP plug-in that operates at the `postSmtpAccept` point of message handling. Messaging Server uses the file `plugins.cfg` to configure the UBE plug-in. A typical UBE configuration in `plugins.cfg` (for a Windows NT installation) might look like this (see Chapter 7, Working With SMTP Plug-Ins, for more information about `plugins.cfg`):

```
PostSmtpAccept i:\Netscape\Server4\msg-Airius1\
   smtp-bin\libUBEfilter.dll
funcs=filter_msg_plugin config=i:\Netscape\
   Server4\msg-Airius1\smtp-bin\plugins\UBEfilter.opt
option=i:\Netscape\Server4\msg-Airius1\smtp-bin\plugins\UBEfilter.opt
```

These command lines tells the server to

- use the file `libUBEfilter.dll` (the library that contains the UBE plug-in)
- call the function `filter_msg_plugin` to start filter processing
- use the filter configuration file named `UBEfilter.cfg`
- use the filter options file named `UBEfilter.opt`

(A Unix version would be similar, except that the paths would be in Unix format and the command line would specify the shared object `libUBEfilter.so`.)

> **Note:** If a plug-in is installed but has been deactivated through the Netscape Console interface, its line in the `plugins.cfg` file is commented out; that is, it starts with a number sign (#) character.

The most important files to note from this `plugins.cfg` example are the filter configuration file and the filter options file. These two files drive the functioning of the UBE plug-in.

- The **filter configuration file** (`UBEfilter.cfg` by default) contains the list of filters to apply to any incoming mail. When you create, edit, delete, activate, or deactivate filters, whether manually or through the Netscape Console interface, you modify this file.
- The **filter options file** (`UBEfilter.opt` by default) controls whether to parse the message header file. You modify this option by editing the file directly or by using the Netscape Console interface (see Parsing Header Fields).

Editing the Filter Configuration File

To create and manipulate UBE filters without using Netscape Console, you need to manipulating several configuration files.

1. Start by ensuring that the UBE plug-in is activated.

   Examine the file `plugins.cfg` (see previous section) to make sure the proper configuration lines are in place to activate the plug-in.

2. If necessary, edit the file `UBEfilter.opt` or its equivalent to specify message-header parsing.

3. Create your set of UBE filters by editing the file `UBEfilter.cfg` or its equivalent. You can use any text editor (Notepad for Windows NT or vi for Unix, for example).

   Enter your filters in order, one per line, in the configuration file. To enter a comment use the # symbol at the beginning of the line. (See Entering Comments for more information on comments.)

4. When you are satisfied with your edits, save the file in its proper location as defined in `plugins.cfg`.

5. To make changes later, open, edit, and resave the configuration file.

During execution, the UBE plug-in processes your filters, in order, from the top to the bottom of the file (except when it encounters a `JUMP` action; see Table 8.1) and applies all rules that match, until it reaches a terminal action or the end of the file.

> **Note:** When you change the configuration file, its new filters automatically take effect immediately.

Omitting Parts of a Filter

All parts of each filter line (other than the optional label) must be present, but you can use empty quotes ("") as a place holder, if you wish to. For example, you can replace the action part of a filter if you want filter processing to continue on the next line, rather than taking action immediately:

```
          Channel-To  (.*)@airius.com  ""
:ceo      $1          ceo              COPY    postmaster@airius.com
```

```
:cfo     $1          cfo             COPY    finance@airius.com
```

In this case, all mail for Airius Corporation is analyzed by subsequent lines to see whether it should be copied to the postmaster or the finance administrator.

For the message field or match-criterion parts of a filter, empty quotes have the effect of matching everything:

```
:cfo     $1          cfo            COPY    finance@airius.com
         ""          ""             JUMP     othermail
```

In this case, once a message has been analyzed to see whether a copy should go to finance, its processing continues with a jump to another location.

Entering Comments

Any line that starts with the number sign (#) or tilde (~) (leading spaces or tabs are ignored) is considered a comment and is ignored during execution by the UBE plug-in.

- You use the number sign (#) to mark comments if you edit the filter file manually. Lines starting with a number sign do not show up in the UBE Configuration form and are not processed during execution.
- The UBE configuration form uses the tilde (~) as a special comment marker. If you disable a filter in the form, the software adds a leading tilde to that filter line in the configuration file. If you enable a previously disabled filter, the software removes the tilde from the line. Both disabled and enabled filters appear in the UBE Configuration form (with their status marked appropriately), but during execution lines starting with a tilde are considered comments and are ignored.

Keep these points in mind when using comment markers:

- Use only the number sign to create comments. The tilde is reserved for use by the UBE Configuration form only.
- Do not use the comment symbol anywhere but at the beginning of a line. Any other location is invalid syntax.

  You can include either the number sign or tilde as a regular character in any part of your filter by enclosing the character in quotes. For example, if you want to filter based on a message field named `X-Accept#`, your filter line could be

```
:Label "X-Accept#" "Free stuff" REJECT "Please don't
send this mail"
```

The following example, however, has invalid syntax:

```
:Label X-Accept# "Free stuff" REJECT "Please don't send
this mail"
```

Examples

Filter examples are shown throughout this chapter as illustrations of filter format. This section provides additional illustrations, including an example of a complexly interacting set of filters that performs many functions.

Example Configuration File

This sample filter configuration file for the fictional XYZ Corporation illustrates filter usage and the interactions among filters. Following the sample are several scenarios illustrating how the UBE plug-in would use this file to handle several kinds of mail.

```
        Channel-To   "louisr@xyzcorp\.com" COPY     "watch@domain.com"
        Subject      "weapons for sale"    DROP     "weap@xxx.gov"
        Channel-To   "CEO.*"               JUMP     "DoCEO"
:xCEO   $#           "50"                  REJECT   "No bulk mail"
        Subject      "May contain a virus" RUN      "VirusScan.exe"
        $&           "1"                   REJECT   "This had a virus"
        Content-Type "multipart/mixed"     JUMP     "DoMime"
        Client       "Netscape.*"         !JUMP     "TstCli"
:xCli   Subject      ".*"                  EXIT
:DoCEO  Subject      "Postmaster Eval"     HOLDCOPY "postmaster eval"
        $ANY         ".*"                  JUMP     "xCEO"
:DoMime Channel-To   ".*_.*@xyzcorp\.com"  REJECT   "Can't read MIME "
        $ANY         ".*"                  EXIT
:TstCli Host-From    ".*\.xyzcorp\.com"    COPY     "IS_department"
        $ANY         ".*"                  JUMP     "xCli"
```

Scenario 1: Message to the CEO for the postmaster to evaluate

These are the received message's `Channel-to` and `Subject` fields:

```
Channel-To: CEO@domain.com
```

```
Subject "Postmaster Eval"
```

1. This message is matched by the `Channel-To "CEO.*"` filter (line 3).

2. Processing therefore jumps to the filter labeled `:DoCEO` (line 10). The filter on that line again matches the message (because the subject is `"Postmaster Eval"`) and so this message is copied to the postmaster, who can then decide whether or not the CEO should see it.

Scenario 2: Message to the CEO about the shareholders' meeting

These are the received message's `Channel-to` and `Subject` fields:

```
Channel-To: CEO@domain.com
Subject "Shareholders meeting"
```

1. As in the previous case, this message is matched by the `Channel-To "CEO.*"` filter (line 3), so processing then jumps to the filter labeled `:DoCEO` (line 10).

2. But this time the filter on line 10 doesn't match the message (the subject is not `"Postmaster Eval"`), so processing passes to the next line (11).

3. The filter on line 11 matches the message (because its predicate can match any string in any field), so processing jumps back to the label `:xCEO` (line 4).

4. At this point the rest of the filters can be applied to this message. If none of lines 4 through 8 match the message, processing will halt with the `EXIT` action at line 9, because the `Subject` fields will match. The mail will then be forwarded to its addressee.

Scenario 3: Message sent to a monitored account:

The account of Louis R. is being monitored for illegal activity. These are the received message's `Channel-to` and `Subject` fields:

```
Channel-To "louisr@xyzcorp.com"
Subject "illegal stock trade"
```

This message is matched by the first filter. A copy of this message is sent to the `watch` account.

Scenario 4: A message arrives addressed to all 3000 employees:

This message is matched by the filter on line 4. That filter automatically rejects any message with 50 or more recipients, regardless of the content of any of its header fields.

Scenario 5: IS requires that all local mail be sent using a Netscape client:

1. If the `Client` field of the message doesn't start with "Netscape", the filter on line 8 transfers processing to the filter labeled `:TstCli` (line 14).

2. That filter tests whether the message was sent from any host in the domain `xyzcorp.com`. If it was, the sender did not use a Netscape client to send the mail, so the plug-in notifies the IS department of that fact by sending them a copy of the message.

3. If the message was not sent locally, processing passes to the last line (15), where it jumps back up to line 9 and continues.

Scenario 6: The account `nomime` can't read MIME messages:

At XYZ Corporation, mail accounts with underscores are reserved for clients that cannot handle MIME attachments. These are the received message's `Channel-to` and `Content-Type` fields:

```
Channel-To r_francisco
Content-Type "multipart/mixed"
```

1. The filter on line 7 matches the content type of the message, so processing jumps to the filter labeled `:DoMime` (line 12).

2. That filter checks the account name. Because the name contains an underscore, the plug-in rejects the mail.

Anti-Relay Example

You can create a set of UBE filters to hinder the practice of *relaying*, the intentional sending of email from an outside domain into your domain when its destination is another outside domain. Mail sent this way is often UBE that is using relaying to hide its original source.

If your installation has a separate external mail server, outside your firewall, that receives external mail but does not forward outbound internal mail, it can effectively stop relaying by examining the `Channel-To` envelope field, like this:

```
Channel-To ".*@xyzcorp\.com" EXIT
$ANY ".*" REJECT "We accept mail for XYZ Corporation only"
```

The first filter passes through any mail destined for the internal domain of XYZ Corporation and then exits. The second filter rejects any mail that does not match the first filter.

If your installation uses the same mail server for both internal and external mail, the filtering requires an extra preliminary step. Add a filter that first checks the source of the message, by looking at the `Host-From` field:

```
Host-From "123.45.67.*" EXIT
Channel-To ".*@xyzcorp\.com" EXIT
$ANY ".*" REJECT "We accept mail for XYZ Corporation only"
```

In this case, the first filter passes through any mail that originates from the subnet belonging to XYZ Corporation and then exits. The second filter passes through any mail that does not match the first filter but is destined for the internal domain of XYZ Corporation. The third filter rejects any mail that does not match either of the first two filters.

> **Note:** Using the same mail server for both internal and external mail is not a recommended configuration. It makes your messaging system more open to external attacks.

Extending the UBE Plug-In

You can extend the UBE plug-in to give it capabilities beyond those delivered with the Messaging Server. Examples in this chapter have already demonstrated one extension method: the use of programs executed by the `RUN` action. Another method of extension involves use of an extension library. This section gives brief overviews of how to implement both methods.

Using the RUN Action

The `RUN` action is built into the UBE plug-in. You can use this action to invoke an external program that can process messages in conjunction with the UBE filters. External programs called in this way can perform tasks such as scanning for viruses, matching message-field content against DNS or other databases of names, matching message-body text, and gathering statistics.

Your external program is executed through a command line that is the argument of the RUN action in a filter.The program provides a return value that a subsequent filter in the configuration file can make use of.

Your program is passed two parameters: the pathname to a file containing the envelope of the message that triggered the RUN action, and the pathname to a file containing the combined header and body of the message. Your program must return a numerical value.

The RUN action is described in Available Actions for UBE Filters.

> Implementing a program executed through the RUN action can be very simple. In many cases, you may be able to use an existing text-manipulation utility, either directly or by writing a simple wrapper that is executed by the RUN action and that in turn calls the text utility.
> **IMPORTANT:** For security purposes, the external program must be located in the same directory of your Messaging Server as the UBE plugin configuration file (*instanceDirectory*/smtp-bin/plugins/).

Using an Extension Library

The UBE plug-in supports use of an extension library that is separate from the plug-in itself. You can write extensions to verify host name, reject relaying, perform DNS lookup, and perform virus checking, and any other task required. An extension library may be more appropriate than a program executed by the RUN action in situations where you want to alter the fundamental nature of a UBE plug-in action, or where you need to add a new kind of action to it.

In Unix environments, the extension library is defined as a shared object or shared library (extension .so or .sl), and in an NT environment it is referred to as a dynamically linked library (extension .dll). In the filter options file you can use the extension_so option to define the path to your shared library. For example, the line

```
extension_so:/lib/HostNameChecker.so
```

instructs the plug-in to load the library HostNameChecker.so into memory.

Basically, an extension library can override existing UBE plug-in actions (such as `COPY` or `EJECT`), and it can also add new actions. If an extension library is present at the time the UBE plug-in reads an action in a filter configuration file, the plug-in takes these steps:

1. It tries to locate the action name in the extension library. If an entry point with that action name is found, the plug-in calls it.
2. If the plug-in finds no entry point with that action name in the extension library, the plug-in executes its own built-in default action.
3. If the plug-in has no built in default action of that name, it does nothing and continues processing the filter configuration file.

Each entry point in the extension library is a function that must use the following prototype:

```
int (*ExtpFuncAct) (
      const char *arg,
      char *control_file,
      char *msg_file,
      int * result
     );
```

where *`ExtpFuncAct`*, the name of the entry point, is the name of the action implemented by this entry point. (That is, `COPY`, `DROP`, `EXIT`, `HOLDCOPY`, `HOLDONLY`, `JUMP`, `REJECT`, `RUN`, or a new action defined by this library.)

The parameters to the function have the following meanings:

`arg`	(input) A pointer to a string that is the argument to the filter action. (The pointer is null if this action takes no argument.)
`control_file`	(input) A pointer to the pathname of a file containing the message's envelope fields.

`msg_file`	(input) A pointer to the pathname of a file containing the message's header fields and body text.
`result`	(output) A pointer to a result code. A return value of 0 indicates that the UBE plug-in should continue processing the filter configuration file; a nonzero return value stops processing filters. This return value is stored in the variable `$&`, which can appear as the message-field name in the subsequent filter in the file. See Special Message-Field Names for more information.

IMPORTANT: When you write an extension library for Unix, be sure to put `extern "C" {}` around your function declaration. (The function name must be text symbols, not C++ symbols. You can verify that fact on most platforms by displaying the library's symbol table with `nm` *`shared_obj`*`.so`, and making sure it's of type `T`.)

Interface Reference: UBE Filters

This section describes the Netscape Console interface elements that allow you to manipulate UBE filters. See *Managing Servers With Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

Unsolicited Bulk Email Configuration Tab

You use the form accessed through this tab to configure the UBE plug-in. For more information, see also

- Creating a New Filter
- Editing an Existing Filter
- Activating and Deactivating Filters
- Changing the Order of Filters
- Envelope Fields and Header Fields

The Unsolicited Bulk Email Configuration form has these elements:

Filters. This field lists, in processing order, all current UBE filters, active and inactive. To edit the content of a filter or to alter its position in the filter list, first select it in this field.

Active. Check this box to make the filter displayed beside it active. If the box is unchecked, the filter is inactive.

Add. Click this button to open the "Add a UBE Filter" window (see Add/Edit UBE Filter Window), which you can use to add a new UBE filter to the current set of filters.

Edit. After selecting a filter in the Filters field, click this button to open the "Edit a UBE Filter" window (see Add/Edit UBE Filter Window), which you can use to edit the characteristics of the selected UBE filter.

Delete. After selecting a filter in the Filters field, click this button to delete the selected filter from the set of UBE filters.

Move up. After selecting a filter in the Filters field, click this button to reposition the selected filter by moving it up one position in the list of UBE filters. This move changes the order in which the filter is processed; when the UBE plug-in runs, it applies filters in sequence from top to bottom.

Move down. After selecting a filter in the Filters field, click this button to reposition the selected filter by moving it down one position in the list of UBE filters. This move changes the order in which the filter is processed; when the UBE plug-in runs, it applies filters in sequence from top to bottom.

Parse message header. Check this box to specify that the UBE plug-in is to analyze the header fields as well as the envelope fields of incoming messages. If this box in unchecked, only envelope fields are matched against the filter criteria. See Envelope Fields and Header Fields for more information.

Action Buttons

Save. Click this button to commit any settings you have made in the Unsolicited Bulk Email form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) describing the Unsolicited Bulk Email form.

Add/Edit UBE Filter Window

You use this window to edit the content of a UBE filter or to add a new filter to your set of UBE filters. For more information, see also

- Creating a New Filter
- Editing an Existing Filter

The Add/Edit UBE Filter window has these elements:

Name (optional). Use this field to enter a label for the filter you are creating or editing. A label is necessary only if this filter is the destination of another filter's `JUMP` action. For more information, see Label.

If. Use this field to select or enter the name of the envelope or header field whose contents this filter is to apply to. You can select one of the common fields from the list, or enter the name of another field. For more information, see Message Field.

=/!=. Click either the "equals" (=) or "does not equal" (!=) radio button. If you click =, the filter action is applied only if the message field matches the criterion; if you click !=, the filter action is applied only if the message field does not match the criterion. For more information, see Negation Modifier.

Value. Use this field to enter the match criterion--a string or regular expression that the filter seeks to match against the contents of the envelope or header field selected in the "If" field. For more information, see Match Criterion.

Case Sensitive. Check this box if you want the matching to be case sensitive. If this box is unchecked, case is ignored. For more information, see case Tag.

Envonly. Check this box if you want this filter to look only at envelope fields. The state of this box matters only if you have checked the Parse header fields checkbox in the UBE Configuration form (see Unsolicited Bulk Email Configuration Tab); if that box is unchecked, all filters look only at envelope fields. For more information, see envonly Tag.

then. Use this field to select the action that this filter is to perform if a match occurs (or if it does not occur, if you have selected the "does not equal" radio button). For more information, see Action.

Argument. Use this field to add any string argument that may be required by the filter action selected in the "then" field. For more information, see Argument.

Action Buttons

OK. Click this button to commit the entries you have made. If you have been creating a new filter, the filter is added to the end of the list of filters. If you have been editing an existing filter, the edited filter replaces the existing version at its current location in the list of filters.

Cancel. Click this button to close the window without making any changes or additions to the UBE filters.

Help. Click this button to display online Help (this document) describing the Add/Edit UBE Filter window.

Chapter

9

Message Routing

This chapter describes how a Netscape Messaging Server receives and delivers a message. This chapter contains the following sections:

- Overview
- Routing Resources
  - The Directory Service
  - The SMTP Routing Table
  - The Domain Name System (DNS)
- How the Messaging Server Routes Messages

Overview

The Messaging Server listens for incoming mail on the standard port for SMTP (port 25). Incoming mail can arrive from either a local mail client or a remote server.

When the Messaging Server receives a message, its Message Transfer Agent (MTA) must determine how to route the message. The routing options include the following:

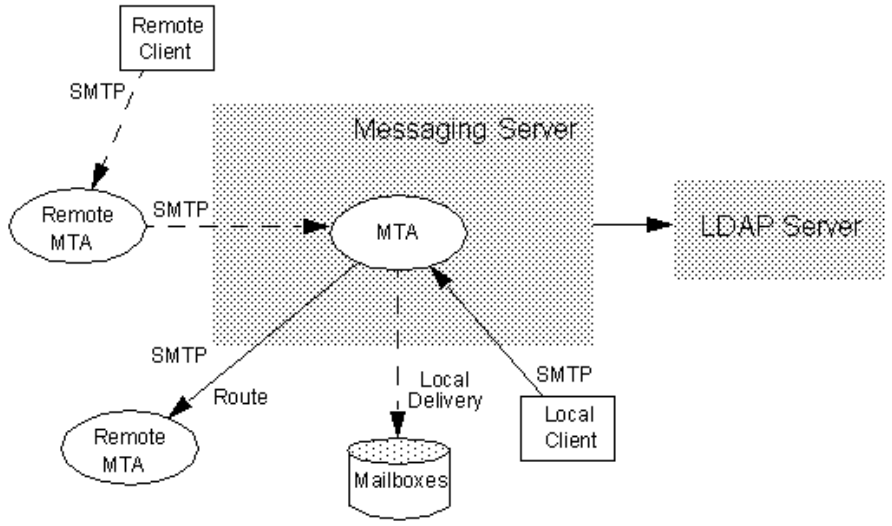
- **Deliver** the message to a local recipient (a mailbox or a program)
- **Route** the message to another MTA (another server)

- **Resend** the message (if the target is a mail group or a forwarded account)
- **Reject** the message (if a recipient address cannot be resolved)

Figure 9.1 shows the routes taken by two messages:

- The dotted lines show a message originating from a remote client and delivered to local mailboxes.
- The solid lines show a message originating from a local client and delivered to a remote messaging server.

Figure 9.1 Mail Routing



Routing Resources

To determine its action, the MTA might reference information from a variety of sources, including the following:

- The Directory Service
- The SMTP Routing Table

- The Domain Name System (DNS)

The MTA checks the directory service to determine if the mail recipient is local or remote. If the recipient is remote, the MTA uses the SMTP routing table and/or the Domain Name System (DNS) server to route the message to another MTA.

The Directory Service

The Netscape Directory Server stores information about the people and resources in your organization. Information about users and user groups is stored in the Directory Server as well as configuration information about the Netscape Messaging Server. Netscape Messaging Server stores information in the Directory Server as LDAP entries to map addresses and route messages.

To route a message, the Messaging Server must determine:

- whether the recipient address has a matching LDAP entry
- whether the recipient address is local or remote
- where to route the message if the recipient address is remote

Each LDAP entry has associated routing and addressing attributes that the MTA uses to determine message delivery or routing options. These attributes are described in Table 9.1. For more information about LDAP object classes and attributes, see the *Netscape Directory Server Schema Reference Manual*.

Table 9.1 Attributes

Addressing	Description
`mail`	Identifies the user's electronic mailing address
`mailAlternateAddress`	Identifies an alternate mail address for the user
Routing	**Description**
`mailHost`	Identifies the host on which the account resides
`mailRoutingAddress`	Identifies the address to place in the envelope when routing a message to this account

The SMTP Routing Table

You can use the SMTP routing table to explicitly specify domains to which the messaging server should direct message processing.

An SMTP routing table entry looks like:

```
*.airius.com:*
```

In this example, messages for any subdomain inside the top-level domain `airius.com` are processed by the receiving messaging server. Thus, if a message addressed to `joe@server1.airius.com` is received by another server inside of `airius.com`, the LDAP resolution of `joe` occurs on that server.

The next example specifies that mail is to be routed to `bigserver` regardless of whether the mail is local or remote:

```
*:bigserver.airius.com
```

The Domain Name System (DNS)

The Domain Name System (DNS) is the naming system that allows computers to find each other on the Internet. Ever computer needs a DNS address to communicate on the Internet. This section provides a brief overview of DNS. For complete details about DNS, see the O'Reilly book, *DNS and Bind, 2nd Edition* by Paul Albitz and Cricket Liu.

The DNS is managed by DNS servers that store information about domains and individual host systems. A DNS server helps the messaging server convert the Internet domain name in an email address into a TCP/IP address. Once the messaging server knows the other computer's IP (Internet Protocol) address, it is able to contact it and forward messages to it.

Each unit of data in the DNS distributed database is indexed by a name. These names are essentially just paths in a large inverted tree, called the domain name space.

A Fully Qualified Domain Name (FQDN) is the unique name that identifies a specific Internet location. FQDNs consist of two or more sections, separated by dots. Each section is a string of letters or numbers without spaces, usually a recognizable word or abbreviation. The order of the sections in an FQDN is significant.

As you move from left to right, each section represents a more general level in the DNS hierarchy. As an example, `yourhost.airius.com`, would refer to a target system `yourhost` at an organization called `airius` which is a subdomain of the top-level domain `com`, which designates it as a company.

The DNS server provides information such as the following to the messaging server:

- Identification of messaging server hosts (for example, what Internet host is supporting mail for this domain?)
- Fully Qualified Domain Name resolution (for example, what is the TCP/IP address for the `airius.com` messaging server?)
- TCP/IP address resolution (for example, what is the name for the address 195.95.92.6?)

DNS Records

DNS servers contain "A" records and "MX" records that are used by messaging servers on the Internet to route email. MX and A records should be entered in the primary DNS server for the domain.

An A record contains a host name and its associated IP address. For example, the following record indicates that the IP address of host `yourhost.airius.com` is `195.95.92.6`:

```
yourhost.airius.com. IN A 195.95.92.6
```

An MX record contains a *mail exchange* that maps a domain name to a host name. For example, the following record indicates that email addressed to anyone at `airius.com` be directed to `server1.airius.com`:

```
airius.com IN MX 10 server1.airius.com
```

The MX record contains two fields: a priority field (`10` in our example) and a host field (`server1.airius.com` in our example). The priority field specifies the priority of this mail exchange (lower numbers have a higher priority). The host field is the name of the mail exchange host.

The exchange host name in the MX record must have at least one A record that maps the host name to an IP address. For example:

```
server1.airius.com IN A 195.95.92.6
```

All DNS queries regarding a specific domain are directed to the DNS server. The primary DNS server uses the MX and A records that have been set up within it to tell querying computers how to route the mail to the local Netscape Messaging Server host.

You can use A records or a combination of A records and MX records to resolve domain names to IP addresses.

Using A Records

You use an A record at the local DNS server to resolve the local Netscape Messaging Server's FQDN to its IP address. For example:

```
server1.airius.com. IN A 195.95.92.6
```

If you are not concerned about security, you can use an A record without an associated MX record.

However, if any of the following are true, you should use an MX record in addition to an A record:

- You are concerned about revealing internal messaging host names on outbound messages.
- You want to hide the internal network configuration.
- You do not want to require senders to know which internal messaging systems users are on.

Using MX Records

Use of MX records in addition to A records is recommended for a messaging service. MX records are used to convert domains that do not point to any particular host into a host name or to route messages for one host to a different host that is running a messaging server.

All messaging servers look for MX records first in their search to identify an external mail host. In addition, MX records establish priority. Priority rankings enable you to identify backup mail servers by inserting additional records in your DNS server. Consider the following example:

```
airius.com IN MX 10 server1.airius.com
```

In this example, inbound messages addressed to `airius.com` (for example `joe@airius.com`, `joe@server1.airius.com`, or even `joe@foobar.sna.foo.servera.server1.airius.com`) are routed to the `server1.airius.com` host; which is assumed to be a messaging server.

The following example provides a backup destination for times when the main destination is unavailable:

```
airius.com IN MX 10 server1.airius.com
airius.com IN MX 20 backupserver.airius.com
```

In this example, mail routed to `airius.com` is routed to `server1.airius.com`. If `server1.airius.com` is unavailable for any reason, messages are sent to an alternate messaging system, named `backupserver.airius.com`.

Remember: Every mail exchange host must have an A record that maps the host name to its IP address.

How the Messaging Server Routes Messages

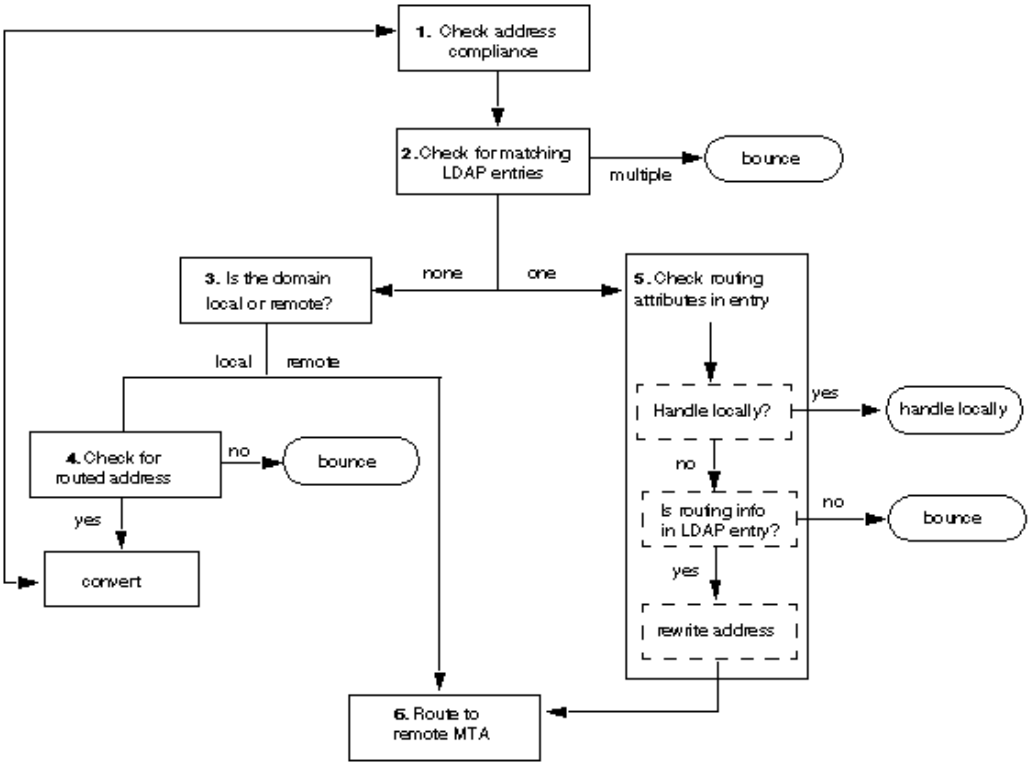
To route a message, the Messaging Server performs the following steps, as described below and shown in Figure 9.2.

1. Check for SMTP address compliance.
2. Search for matching LDAP entries. If no match is found, proceed to Step 3; if one match is found, proceed to Step 5.
3. Check to see if the domain is local or remote. If domain is local, proceed to Step 4. If domain is remote, proceed to Step 6.
4. Check for routed address. If none, bounce the message. Otherwise, proceed to Step 1.

5. Check routing attributes in LDAP entry.

6. Route to remote MTA.

Figure 9.2 Routing Diagram



Step 1: Check SMTP Address Compliance

The Messaging Server requires standard, fully qualified SMTP addresses in the `RCPT TO:` field of the message envelope (for example, `joe@domainname.ext`).

If a message envelope does not have a fully qualified SMTP address (for example, `joe`), the Messaging Server attempts to make the address standard by adding the domain to the address as follows:

1. If the Address Completion Domain field has been defined, the Messaging Server uses the value found in the LDAP entry.
2. If the Address Completion Domain field has not been defined, the Messaging Server appends its `serverhostname.domainname.ext` to the envelope address (for example, `joe@serverhostname.domainname.ext`).
3. If the address is of the form `joe@server`, the Messaging Server appends its `domainname.ext` extension to the envelope address (for example, `joe@server.domainname.ext`).
4. If the address includes an IP address, such as `joe@198.93.93.10`, the Messaging Server will perform IP address resolution and replace the IP address with the matching host name (for example, `joe@gethost`).

Step 2: Search for matching LDAP Entries

The Messaging Server searches for an LDAP entry with a `mail` or `mailAlternateAddress` attribute that matches the envelope recipient address.

The search includes only LDAP entries that 1) have object class `mailRecipient` or `mailGroup` and 2) are in the directory subtree specified by the configured Base DN.

- If a matching address is found, the Messaging Server proceeds to Step 5.
- If multiple matches are found, the Messaging Server assumes the address is invalid, treats it as unknown, and rejects the message.
- If no match is found, the Messaging Server proceeds to Step 3.

Alternate Search Methods

If an exact match for an address is not found, you can expand the list of possible matches by specifying one or more of the following search methods. If all search methods are specified, the server tries each method in the order listed until a match is found:

- Search for custom domain
- Search using truncated domain
- Search by user ID

The default setting is search by user ID.

Note: Specifying alternate search methods has a slight impact on performance.

Search for custom domain. Assume Joe has two addresses with his ISP: `joe@isp.com` and a custom domain address, `joecorp.com`. To enable Joe to receive mail addressed to *`anything`*`@joecorp.com`:

1. Add a `MailAlternateAddress` value for Joe as follows: `@joecorp.com`.
2. Add MX records in DNS as necessary to specify the messaging server for the custom domain.

Search using truncated domain. In a network environment, you might want the option of ignoring the host name when searching for an address. For example, assume the following:

- The value for `MessageHostName` is `foo.airius.com`
- Joe's email address is `joe@airius.com`

With this feature enabled, the server can ignore the host name `foo` when searching in the directory for the correct address. Consequently, Joe can receive messages addressed to both `joe@foo.airius.com` and `joe@airius.com`.

Note: Use this feature only if user accounts are not specific to a particular host. For example, if `user@host1.domain.com`, `user@host2.domain.com`, and `user@domain.com` are considered different accounts, do not enable this feature.

Search by user ID. The server can search on the user ID if the domain in the address matches one of the host values specified for the `MessageHostName` parameter or if the domain is configured as a local mail domain.

With this feature enabled, each user's `uid` attribute in LDAP is a valid email address for that user in an address such as `uid@LocalMailDomain` or `uid@MessageHostName`.

Note: Do not use this feature if you do not want the user's `uid` to be treated as a valid email address.

Step 3: Check if Domain is Local or Remote

The Messaging Server considers the address local if the domain part of the address matches:

- The name of the host on which the Messaging Server resides
- The address completion domain setting (if set)
- A local domain setting (if set)

If the domain is local, the Messaging Server proceeds to Step 4. Otherwise, the Messaging Server considers the address to be remote and proceeds to Step 6.

Step 4: Check for Routed Address

The Messaging Server checks to see if the recipient address is a routed form (for example, `local%domain1@domain2`). If the recipient address is a routed address, the Messaging Server rewrites the address as `local@domain1`. The rewritten address is considered a new address, so the Messaging Server proceeds to Step 1. If the recipient address is not a routed address, the message is bounced.

Step 5: Check Routing Attributes

If an LDAP entry matches the address, the Messaging Server checks the routing attributes for the address and takes the following actions:

- If the LDAP entry contains a `mailHost` attribute, the Messaging Server will deliver or route the message to the server specified by the attribute:
  - Local Server. If the `mailHost` attribute indicates the local server, then the entry's `uid` attribute is used for local delivery and the Messaging Server handles the message locally.
  - Remote Server. If the `mailHost` attribute indicates a remote server, the local MTA rewrites the address and routes the message to the remote MTA as described in Step 6. See Rewrite Address for Routing to Remote MTA for more information about rewriting the address.
- If the LDAP entry does not contain a `mailHost` attribute, but does contain an enabled `mailRoutingAddress` attribute, the Messaging Server rewrites the address and proceeds to Step 6 to route the message. See Rewrite Address for Routing to Remote MTA for more information about rewriting the address.
- If the LDAP entry contains no routing information (that is, no `mailHost` attribute and no enabled `mailRoutingAddress` attribute) but specifies that the account is a mail group or a forwarding-only account, then the message is handled locally.
- If the LDAP entry contains no `mailHost` attribute and cannot be routed or handled locally, the Messaging Server rejects the message.

Rewrite Address for Routing to Remote MTA

If the recipient was found in LDAP, but the `mailHost` attribute in the LDAP entry is not this server, the Messaging Server then tries to route the message to a remote MTA. The Messaging Server administrator can specify whether and how the server rewrites the envelope recipient address before routing the message to the remote MTA.

Note: The envelope address is rewritten only if the intended recipient was found in LDAP and is not local. (The server rewrites the envelope recipient address in the SMTP protocol dialog.).

The administrator can specify one or more of the following methods. By default, these methods are disabled. The server tries each enabled method in the order listed until it is able to compose a new address using the indicated attributes from the account's LDAP entry:

- Use the `mailRoutingAddress` attribute
- Combine the `uid` with the `mailHost` attribute
- Combine the local part of the address with the `mailHost` attribute

If the server is unable to compose a new address (because the necessary attributes are not present in the user's LDAP entry or because no search methods are selected), the envelope address is not changed. However, if the "search by truncated domain" method was attempted in step 2, the truncated address is used instead of the original address.

The default method is to use the original address unmodified.

mailRoutingAddress Attribute

The `mailRoutingAddress` attribute method specifies a specific mail routing address. This method is most useful for LDAP entries that represent mail accounts on non-Netscape mail servers or gateway systems.

You must also modify the user's LDAP entry (by using `ldapmodify`) to include the `mailRoutingAddress` attribute. For example:

```
mailRoutingAddress: joesmith@judge.airius.com
```

The `mailRoutingAddress` attribute differs from the `mailForwardingAddress` attribute as follows:

- `mailRoutingAddress` determines how to route the message to the server that handles this account (the mail account that is represented by this LDAP entry)
- `mailForwardingAddress` determines how a mail account forwards its mail to some other account

Combine uid and mailHost Attributes

This method combines the `uid` attribute and the `mailHost` attribute found in the LDAP directory.

For example, mail arrives on one server for `Joe_Smith@airius.com`. The server determines that this mail belongs to `jsmith` whose mail account is on `judge.airius.com`. The server rewrites the envelope address to `jsmith@judge.airius.com` then relays the message to `judge.airius.com`.

This method works best if the "search by user ID" method is employed on the next server.

Note: Some sites prefer that only explicit addresses (those specified by the `mail` and `mailAlternateAddress` attributes) are valid email addresses for users. You should not use this method if the local policy does not consider `uid` a valid email address.

Combine Local Part and mailHost Attribute

This method combines the local part of the original address with the `mailHost` attribute value to create the new address. For example, `Customer_Service@airius.com` becomes `Customer_Service@judge.airius.com`. This method is useful to support entities, such as mail groups, that do not have a `uid`.

Note: This method is not used if the "custom domain" search method was used to resolve the address.

Some SMTP installations prefer that addresses routed internally within the network be host-specific. This feature is most likely to work properly if the "truncated domain" search method is in use on the next server, or if all user accounts have a matching email address explicitly specified.

Do not use this method unless, for each address of each user (as specified with the `mail` and `mailAlternateAddress` attributes), changing the domain part to a specific host does not create ambiguity about the message recipient. For example, suppose the mail server `mail5.airius.com` has three different users: `joe@division1.airius.com`, `joe@division2.airius.com`, and `joe@airius.com`. In this scenario, `joe@airius.com` would receive mail addressed to the other users, if the "local part at mailHost" rewrite method is used on the sending MTA and the "truncated domain" search method is used on `mail5.airius.com`.

Step 6: Route to Remote MTA

At this point, the Messaging Server assumes another mail server is responsible for this recipient. Two steps are taken to direct the delivery to a remote MTA:

1. Check SMTP routing table
2. Check Domain Name Server (DNS) definition for recipient domain
    - Use MX records if present
    - Otherwise, use A records

Check SMTP Routing Table

The Messaging Server checks its SMTP routing table to see if mail for the recipient's domain should be routed to a specific mail server host.

- If the routing information includes a TCP/IP address, the Messaging Server delivers the mail to the remote host.
- If the routing information does not include a TCP/IP address, but specifies a host or domain name, the Messaging Server asks its host machine to find the TCP/IP address of the mail server for that domain. See Check Domain Name Server Definition or Local Host Files for more information.

Note: Entries in the SMTP routing table are processed in order. You should keep this in mind when creating entries. For example, if you have a route entry that sends all non-local mail to a firewall mail server, you would want this entry to be the last entry in the routing table.

Example Routes

The following example routes all internal mail through a hub server:

```
*.airius.com:hub.airius.com
```

The next example forces the use of IP addresses for frequently called servers (bypassing DNS):

```
hub.airius.com:[123.345.456.7]
```

The next example shows the use of a firewall server for all outside mail:

```
*airius.com:*
```

```
*:firewall.airius.com
```

Check Domain Name Server Definition or Local Host Files

If the route specified in the SMTP routing table does not contain a TCP/IP address, the Messaging Server assumes it should deliver the mail message to the domain's mail server as defined by the host's specified Domain Name System.

The Messaging Server asks its host machine to find the TCP/IP address of the mail server for that domain. To find the TCP/IP address of the remote mail server, the Messaging Server host machine performs the following steps:

1. Asks for the Mail Exchange Record (MX record) defined for that domain and if found returns the TCP/IP address of that mail server.

2. If no MX record is found, the host asks for the Address Record (A record) for that domain name and if found returns the TCP/IP address of that host.

3. If no MX or A records are found for that domain name, the host checks its local host file (depending on the system's host name lookup configuration) to see if the domain name might be listed with a TCP/IP address.

If the Messaging Server finds a TCP/IP address, the server delivers the message to that address.

If the Message Server does not find a TCP/IP address for that domain name, the message is considered undeliverable and the Messaging Server generates an error message that is delivered to the Postmaster and the originator (if specified in the Messaging Server configuration forms).

Chapter

10

Monitoring and Maintaining Your Server

After you install and configure Netscape Messaging Server, you need to perform various tasks to monitor and maintain your server. Many of these tasks are performed automatically by the server. For example, the `stored` utility performs daily maintenance tasks for the server, such as erasing messages stored on disk according to expiration policies you specify. This chapter contains the following sections:

- Overview
- Performing Daily Tasks
- Monitoring and Controlling Disk Usage
- Monitoring Server Response Time
- Performing Recovery Tasks
- Factors Affecting Messaging Server Performance
- System Monitoring Tools
- Using SNMP

Overview

In most cases, a well-planned, well-configured server will perform from day to day and from month to month without requiring intervention from an administrator. As an administrator, however, it is your job to monitor the server for exception conditions that require action on your part to keep the server running smoothly. Tasks you should perform include:

- monitoring disk usage
- monitoring server performance and response times
- managing exception conditions when and if they occur
- reconfiguring, when necessary, to accommodate new users or new conditions

This chapter focuses on Messaging Server configuration and maintenance. However, you will also need to monitor the system on which the server resides. A well-configured server cannot perform well on a poorly-tuned system. For example, you should monitor the following conditions:

- CPU performance
- disk I/O
- memory usage
- network performance

This chapter does not provide details about system monitoring and performance. However, it does provide information about tools you can use to monitor system performance; see System Monitoring Tools.

Netscape Messaging Server 4.0 provides several command-line utilities for monitoring and maintaining your server, as described in Table 10.1. For complete syntax reference and usage guidelines for these utilities, see Appendix A, Command-line Utilities.

Table 10.1 Command-Line Utilities

Category	Command-Line Utility
Management	`configutil, imscripter, mboxutil, NscpMsg, processq`
Recovery	`deliver, reconstruct`

Table 10.1 Command-Line Utilities

Category	Command-Line Utility
Background and daily tasks	`stored`
Monitoring and reporting	`counterutil, hashdir, mailq, quota, readership`

Performing Daily Tasks

Probably the most important tasks you should perform on a daily basis are checking the `postmaster` account and monitoring the log files.

Checking the postmaster Account

The Messaging Server has a predefined administrative alias account set up for the postmaster. The `postmaster` account is defined in RFC822, which requires every email site to accept mail addressed to a user named `postmaster` and that mail sent to this account be delivered to a real person. All messages sent to `postmaster@host.domain` are sent to this account.

Typically, the `postmaster` account is where users should send email about their mail service. You might receive mail from local users about server response time, from other server administrators who are encountering problems sending mail to your server, and so on. *You should check this account daily*.

You can also configure the server to send certain error messages to the `postmaster` account. For example, when the MTA cannot route or deliver a message, you can be notified via email sent to the `postmaster` account. You can also send exception condition warnings (low disk space, poor server response) to the `postmaster` account. For more information about sending messages to the `postmaster` account, see Specifying Error Handling in Chapter 3 and Alarm Attributes in Appendix A.

Monitoring and Maintaining the Log Files

Netscape Messaging Server creates a separate set of log files for each of the major protocols, or services, it supports: SMTP, IMAP, and POP. You should monitor the log files on a routine basis--especially if you are having problems with the server. For information about searching and viewing log files, see Searching and Viewing Logs in Chapter 11.

Be aware that logging can impact server performance. The more verbose the logging you specify, the more disk space your log files will occupy. You should define effective but realistic log rotation, expiration, and backup policies for your server. For information about defining logging policies for your server, see Defining Log Rotation, Expiration, and Backup Policies in Chapter 11.

Setting Up the stored Utility

The `stored` utility performs automatic monitoring and maintenance tasks for the server, such as:

- background and daily messaging tasks
- low-level database consistency check and repair
- deadlock detection and rollback of deadlocked database transactions
- cleanup
- expiration, expunging, and erasing of messages stored on disk
- alarm setting

The `stored` utility automatically performs cleanup and expiration operations once a day at midnight. You can choose to run additional cleanup and expiration operations; for example, to run `stored` as a daemon once a day at 09:00 p.m., type the following command at the command line:

```
stored -d -h 21
```

For more information about `stored`, see `stored` in Appendix A and Using the stored Utility in Chapter 5.

Monitoring and Controlling Disk Usage

The server requires adequate disk space for processing and storing messages. You must never let the server run out of disk space. Consequently, you must monitor disk usage and take appropriate actions if available disk space becomes too low.

The message queue contains messages that cannot be routed or delivered immediately. The message store contains the messages delivered to local users. Both the queue and the store must have adequate disk space for the messages they contain. For example, if disk space reserved for the store falls too low, the server might start queueing messages destined for the store. If disk space reserved for the queue falls too low, the server might start rejecting messages. For general information about the message queue, see Managing the Message Queue in Chapter 3. For general information about the message store, see Chapter 5, Managing the Message Store.

Monitoring Disk Usage

You can monitor disk usage by configuring the disk space alarm attributes described in Table 10.2. You configure these attributes by using the `configutil` utility. You can specify how often the system should monitor disk space and under what circumstances the system should send a warning.

Table 10.2 Disk Space Alarm Attributes

Disk Space Attributes	Default Value
`alarm.diskavail.msgalarmstatinterval`	3600 seconds
`alarm.diskavail.msgalarmthreshold`	10%
`alarm.diskavail.msgalarmwarninginterval`	24 hours

For example, if you want the system to monitor disk space every 600 seconds, specify the following command:

```
configutil -o alarm.disavail.msgalarmstatinterval -v 600
```

If you want to receive a warning whenever available disk space falls below 20 %, specify the following command:

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

For more information about setting alarm attributes, see Appendix A, Command-line Utilities.

Controlling Disk Usage

You can control disk usage by setting user message quotas, specifying aging policies for messages stored on disk, limiting the size of messages the server will accept, and processing the message queue at frequent intervals. If these methods are not sufficient or are not acceptable to your users (or are not practical), you might want to consider adding disks to your system. For more information, see Specifying Alternate Paths for Queue Storage in Chapter 3 and Configuring Message Store Partitions in Chapter 5.

Message Quotas

If disk space is limited, you might want to set user message quotas for your system. Message quotas allow you to limit users to a fixed mailbox size. If a user exceeds the limit, the user can no longer retrieve mail until he or she deletes existing messages to free disk space. For information about specifying message quotas, see Configuring User Disk Quotas in Chapter 5.

You can use the `quota` utility to view reports and optionally fix mailbox quota usage. This utility generates a report listing quotas, giving their limits and usage. For more information about the `quota` utility, see Appendix A, Command-line Utilities.

Aging Policies

Another method for controlling disk space is to specify aging policies for messages in the message store. You can control how long messages are stored in one or more mailboxes. If you set aging policies, you should educate your users about these policies because the server will not send a warning message before it starts deleting messages from the store.

You can specify constraints for the following:

- number of messages in the mailbox
- total size of the mailbox

- number of days that messages remain in the mailbox
- number of days that messages exceeding a given size remain in the mailbox

For more information, see Specifying Aging Policies in Chapter 5.

Message Size Limits

You might want to limit the size of messages that your server will accept. If you limit message size, the server will automatically reject any messages that exceed the maximum message size. By limiting the size of messages, you'll save queue disk space and message store disk space. For more information about how to limit message size, see Limiting Message Size (SIZE) in Chapter 3.

Reserved Disk Space

You can specify a minimum amount of disk space that will remain unused for the message queue. If the minimum threshold is reached, the server will temporarily reject all messages until disk space is freed. The server returns an error (452) notifying the client of a temporary disk space shortage and asking the client to resend the message at a later time. For information about how to reserve free disk space, see Reserving Free Disk Space in Chapter 3.

Monitoring Server Response Time

In general, server response time is measured by the number of messages per second and the number of client connections per second your server can handle. There are many factors that affect server response time: number of users, peak traffic times, hardware and software configuration, network bandwidth, and so on.

The `msgalarmproc` utility provides a set of server response attributes you can use to monitor server response time for IMAP, POP, and SMTP services. These attributes are listed in Table 10.3. Response time is measured for how long it takes to make a connection to a service and to receive the service greeting. If response time exceeds a specified number of seconds, you will be notified via email. You set values for the server response attributes by using the `configutil` utility. For more information about the `configutil` utility and the `msgalarmproc` attributes, see Appendix A, Command-line Utilities.

Table 10.3 Server Response Attributes

Server Response Attributes	Default Value
`alarm.serverresponse.msgalarmstatinterval`	600 seconds
`alarm.serverresponse.msgalarmthreshold`	10 seconds
`alarm.serverresponse.msgalarmwarninginterval`	24 hours

To improve server response time, you can:

- Run `stored` at off hours--not during peak hours for your business.
- Defer queue processing to off hours.
- Reduce the size of the queue.
- Distribute the queue across multiple physical disks.
- Distribute the message store across multiple physical disks.
- Limit the size of user inboxes.

For more information about improving server response time, see Factors Affecting Messaging Server Performance later in this chapter.

Performing Recovery Tasks

If one or more mailboxes becomes corrupt, you can use the `reconstruct` utility to rebuild the mailboxes or the mailboxes database and repair any inconsistencies. For more information, see Repairing Mailboxes and the Mailboxes Database in Chapter 5.

For information about backing up and restoring the message store, contact your Netscape technical support person.

Factors Affecting Messaging Server Performance

This section describes factors that affect Messaging Server performance and contains tips to help you enhance the performance of Netscape Messaging Server 4.0 on Unix platforms. These tips are intended as general guidelines and suggestions only; the actual performance of your messaging server depends on many factors, including CPU power, disk space, usage patterns, network bandwidth, and so on.

Note: The tips in this document are for Netscape Messaging Server 4.0 only and might or might not apply to other versions of Netscape Messaging Server.

Factors that affect Netscape Messaging Server performance include the following:

- Number of Users per Disk
- Configuration of POP and IMAP Services
- Configuration of SMTP Services
- Configuration of Logging Services
- Size of Mailboxes
- Distribution of the Store and Queue Directories
- MTA Thread Settings
- Applications Co-Resident with the Messaging Server
- Activity of the Administration Server
- Activity of the Directory Server
- Location of the Messaging Server and the Directory Server
- Number of Address Lookups per Message
- Ratio of Delivery to Outbound Sends
- Use of RAID Technology
- Memory, Disk, and CPU Requirements

Number of Users per Disk

As the number of users per disk increases, the I/O to that disk increases non-linearly due to the algorithms used by the OS to cache the directory index (it's faster to search memory than to search a hard drive). To improve disk access, you should distribute users across available disks.

To ease management of multiple disks, you can use RAID (Redundant Array of Inexpensive Disks) technology to distribute data across a series of physical disks. For more information, see Use of RAID Technology.

Configuration of POP and IMAP Services

How you configure your POP and IMAP services affects Messaging Server performance. You can configure the following:

- the number of POP and IMAP processes
- the number of POP and IMAP connections per process
- the number of threads per POP and IMAP process

For details on configuring POP and IMAP services, see Chapter 2, Configuring IMAP and POP Services.

Number of POP and IMAP Processes. If you have a multiprocessor machine, you might want to configure multiple POP and IMAP processes to allow more connections to your server and perhaps less thread contention. There is a performance overhead, however, in allocating tasks among multiple processes and in switching from one process to another.

Number of POP and IMAP Connections Per Process. IMAP connections are generally very efficient compared to POP connections. Each reconnection during a POP session requires re-authentication of the user, whereas an IMAP connection requires only a single authentication because the connection remains open.

Scalability is most adversely affected, therefore, by the number of POP users "pinging" the server to see if they have new mail. Netscape Messaging Servers can service several dozen user requests per second. Consequently, 10,000 POP users checking mail once a day is easier to support than 1000 POP users checking mail every second during the day.

Connected processes do occupy memory on the server system, however. Because IMAP connections are persistent, the more IMAP users there are connected to the server, the fewer resources there are for new connections.

Number of Threads per POP or IMAP Process. Having more simultaneously executing threads means that more client requests can be handled without delay, so that a greater number of clients can be serviced quickly. However, there is a performance overhead to dispatching among threads, so there is a practical limit to the number of threads the server can make use of.

Configuration of SMTP Services

This section summarizes SMTP configuration options that affect system performance. Some of these options can improve server performance; other options provide valuable features but can impact server performance adversely. If you are having problems with server performance for whatever reasons, you might want to consider whether you need the features provided by some of these options. SMTP configuration options that can affect server performance include:

- Limiting Dial-up Connections
- Limiting the Size of Messages
- Verifying Recipient Addresses
- Enabling Host Name Resolution
- Specifying Alternate Search Methods
- Specifying "From" Address Rewrite Style
- Using the Plug-in API

Limiting Dial-up Connections

You can improve server performance by limiting the number of dial-up connections to your server. If both client (in this case another MTA) and server support the ETRN command, when the client connects to the server to send a message, it can also initiate processing of the deferred queue for the client's domain. This feature is useful for sites that only have a dial-up connection to the Internet. For more information, see Enabling Requests for Deferred Queue Processing (ETRN) in Chapter 3.

Limiting the Size of Messages

The size of messages is a factor when considering the transmit time to actually "move" the message from the client to the server and the disk space available for storing messages. Users may negatively impact performance by sending extremely large documents over the network. You can limit the size of messages your server will accept. For more information, see Limiting Message Size (SIZE) in Chapter 3.

Verifying Recipient Addresses

You can specify an option to verify recipient addresses when a client connects to the server. Specifying this option has slight performance impact because the server must perform an LDAP lookup for each recipient while connected to the client. The benefit, however, is that bad recipients can be rejected immediately, allowing the sender to fix before sending (instead of getting a bounce message later). For more information, see Verifying Recipient Addresses in Chapter 3.

Enabling Host Name Resolution

If you enable this option, the Messaging Server will use DNS to map the client's IP address to the associated host name. The host name is then used in the process table, the log files, and in "Received" lines in message headers. This option requires DNS lookups, however, so enabling this option can impact performance adversely if your server handles a large volume of messages. For more information, see Performing Host Name Resolution in Chapter 3.

Specifying Alternate Search Methods

If you enable alternate search methods, you can expand the list of possible recipient matches. Be aware that enabling this option can impact server performance because of the increase in LDAP lookups. For more information, see Specifying Alternate Search Methods in Chapter 3.

Specifying "From" Address Rewrite Style

Rewriting the "From:" address increases the odds that replies to outgoing messages are processed correctly. However, this feature does incur some performance overhead. For more information on this option, see From Address Rewrite Style in Chapter 3.

Using the Plug-in API

If you are using the Messaging Server plug-in API, some CPU and memory resources will necessarily be diverted from the usual Messaging Server processing. However, you can use the plug-in API to provide valuable extensions to the Messaging Server capabilities. For more information, see Chapter 7, Working With SMTP Plug-Ins.

Configuration of Logging Services

Logging options can be expensive in terms of server performance and response time. You should carefully consider your logging requirements and log only those messages that you need to successfully monitor and maintain your server. For more information on logging policies, see Defining Log Rotation, Expiration, and Backup Policies in Chapter 11.

Size of Mailboxes

Users with mailboxes that contain an extremely large number of messages might encounter slow response times from the server. If so, you might want to set up user disk quotas or aging policies for user mailboxes. For more information about disk quotas and aging policies, see Chapter 5, Managing the Message Store.

You might also want to consider distributing mailboxes across disks. See Distributing the Store Across Disks.

Distribution of the Store and Queue Directories

The `store` directory contains the user mailboxes. The `queue` directory is a temporary directory where all mail manipulation and rewriting take place. To improve disk access, the `store` directory and the `queue` directory should reside on separate disks. If you have a fast RAID setup (see Use of RAID Technology), you should keep the store and the queue on separate disks, but on the same logical volume. You should also consider:

- Mounting the Queue Directory on a Fast File System and Fast Disk
- Distributing the Queue Across Disks
- Distributing the Store Across Disks

To ease management of multiple disks, you can use RAID (Redundant Array of Inexpensive Disks) technology to distribute data across a series of physical disks. The disks appear as one logical volume, so disk management is simplified. For more information, see Use of RAID Technology.

Mounting the Queue Directory on a Fast File System and Fast Disk

Because the message queue directory is the most heavily used part of the system, you should mount the queue directory on a very fast file system, such as the Veritas file system (VsFS). Mounting the queue directory on a fast file system can significantly increase performance for SMTP accept rates. By maintaining the queue directory in its own file system, you can also monitor message queue performance separately from message store performance.

You should also consider disk performance. For example, newer I/O buses like Ultra2 SCSI and Fibre Channel can transfer large quantities of data rapidly—up to 80 MB per second. The faster the communication speed between disk and CPU, the better Messaging Server will perform.

Distributing the Queue Across Disks

If you have more than one disk available, you might want to distribute the queue across disks. By distributing the queue, you can reduce the load associated with delivering a message because the server can perform concurrent I/O operations. You can also use multiple queue directories to reduce the overhead associated with large number of files accumulating in a single queue. For more information about specifying alternate queues, see Specifying Alternate Paths for Queue Storage in Chapter 3.

Distributing the Store Across Disks

For improved mailbox access performance, you can distribute the message store across multiple disks. When distributing the message store, you should limit the number of mailboxes on any one disk.

Distributing mailboxes across disks does not change the SMTP access rate, but it will dramatically improve message delivery time. The number of mailboxes you allocate per disk depends on the following factors:

- disk capacity
- disk space allocated to each user

Note: Messaging Server 4.0 stores one copy of each message per file system. Therefore, if you have 5 disks, each disk will contain a copy of the message.

For more information about distributing the message store, see Configuring Message Store Partitions in Chapter 5.

MTA Thread Settings

You can use the `configutil` utility to modify the thread settings for various MTA components:

```
service.smtp.account-handler.minruncount
service.smtp.autoreply-handler.minruncount
service.smtp.error-handler.minruncount
service.smtp.mailbox-deliver.minruncount
service.smtp.prog-deliver.minruncount
service.smtp.smtp-accept.minruncount
service.smtp.smtp-deliver.minruncount
service.smtp.smtp-router.minruncount
service.smtp.unix-deliver.minruncount
```

For example, you might want to improve the SMTP acceptance rate and allow for more simultaneous inbound connections by increasing the number of threads allocated to the `service.smtp.smtp-accept` component as follows:

```
configutil -o service.smtp.smtp-accept.minruncount -v 300
```

As another example, you might want to improve the mailbox delivery rate by increasing the number of threads allocated to the `service.smtp.mailbox-deliver` component as follows:

```
configutil -o service.smtp.mailbox-deliver.minruncount -v 10
```

Be aware that threads use available memory. So, depending on the hardware configuration of the server machine, too many threads can impede server performance.

Applications Co-Resident with the Messaging Server

Be aware that other applications running on the same system as Netscape Messaging Server will compete for the same system resources (memory, disk space, and so on) as the Messaging Server. Depending on your messaging requirements, you might want to dedicate one or more machines to the messaging services.

Activity of the Administration Server

If the Netscape Administration Server is being used while Netscape Messaging Server is running, there will be less memory available to map incoming connection requests.

Activity of the Directory Server

If the Messaging Server is competing with numerous other LDAP clients (for example, other Netscape servers or a synchronization process with another LDAP based directory) for access to the Directory Server, Messaging Server performance will be affected. Under large stress loads (greater than 5000 local entries), you should replicate the directory services to more machines to increase accessibility of the service. You should also dedicate a directory machine to one or more Messaging Servers.

Location of the Messaging Server and the Directory Server

In general, for improved performance, you should keep the Messaging Server and the Directory Server on separate machines. Placing these servers on separate machines will prevent contention over system resources (CPU, RAM, and disk space).

If you do decide to place the servers on separate machines, you must also consider the network bandwidth between the two machines. For example, a 100 MB dedicated network should provide good performance. If possible, you should consider using full duplex on a switch/dedicated network to eliminate collisions.

Number of Address Lookups per Message

Be aware that if the average message is destined for a large number of recipients, there is a corresponding increase in the number of required LDAP lookups required to resolve the address. You might want to limit access to aliases that contain a large number of users; for example, you might not want all users to have access to the `companyall` alias.

Ratio of Delivery to Outbound Sends

Most customers have a higher number of messages received to messages sent per user (on the order of 4 to 1 or higher). Netscape messaging solutions are optimized for exactly these kind of environments. Because sending a message on the server is more "expensive" than receiving, any deviation from the expected ratio (for example, 1:1 sending and receiving) will affect the expected performance and scalability of your Messaging Server.

Use of RAID Technology

To ease management of multiple disks, you can use RAID (Redundant Array of Inexpensive Disks) technology to distribute data across a series of physical disks. With RAID technology, multiple disks appear as one logical volume, so disk management is simplified. You can have multiple logical volumes each consisting of several physical disks.

There are several levels of RAID technology. You should consider implementing a RAID-0+1 configuration. RAID 0 provides fast access to data through a technology called striping. A stripe is a disk segment varying in size from one sector up to several megabytes. Disk I/O is distributed across all stripes. RAID 1 implements disk mirroring for fault tolerance.

Memory, Disk, and CPU Requirements

As stated before, a well-configured server cannot perform well on a poorly-tuned system. During the initial planning stage, you need to estimate your memory, disk, CPU, and network bandwidth requirements for your business environment. These estimates depend on many factors, including how many users the server supports, average number of messages per user, geographic location of users, and so on.

Of course, your estimates will depend on usage patterns and mail configuration. For example, if you are a host providing resources to residential consumers, your estimates will differ from the estimates required for corporate use. In general, residential consumers use much less resources than corporate consumers, so you would allocate less memory, disk space, and processing power for each residential user.

If your original estimates did not plan for growth, if business conditions change, or if performance requirements change, you might need to reconfigure your hardware. For example, you might need to add disks to the system, add processors, and so on. Although deployment planning is beyond the scope of this section, you can use the tools described in System Monitoring Tools to monitor how your system is performing.

System Monitoring Tools

The following table lists system tools you can use to monitor your server environment. These tools are available on various Unix platforms. For more information about these tools, see the man pages delivered with your Unix system.

Table 10.4 General Unix Tools

Tool	Description
`iostat`	Provides information about disk I/O and CPU usage.
`lsof`	Provides information about open file descriptors. (Available in source from :ftp://vic.cc.purdue.edu/pub/tools/unix.)
`lslk`	Provides information about file system locks. (Available in source from :ftp://vic.cc.purdue.edu/pub/tools/unix.)
`netstat`	Provides statistics about network functions.
`nslookup`	Allows you to query DNS servers for information about hosts and domains; for example you can print a list of hosts in a particular domain; also provides an IP address-to-hostname mapping function (and vice versa).
`ping`	Allows you to query the status of a remote host or network gateway.
`sar`	Unix SysV performance monitoring tool. Useful for gathering system information over a longer period of time to use in long term planning, for example.
`tcpdump`	Public domain tools used in debugging and to monitor network traffic.
`top`	Provides quick, easy monitoring of processes and CPU activities. (This is a public domain tool that works on most Unix platforms.)
`trace`	Similar to `truss` on Solaris. Sometimes included by the vendor; otherwise, you can download this tool from an Internet site.

Table 10.4 General Unix Tools

Tool	Description
`traceroute`	Determines the path a packet takes throughout the Internet to reach its final destination.
`vmstat`	Provides statistics about process, virtual memory, disk, trap, and CPU activity.

Table 10.5 System Monitoring Tools - Sun Solaris

Tool	Description
`lockstat`	Provides information on OS and application locking. Available on Solaris 2.6 only.
`mpstat`	Provides statistics about each processor on the system
`pmap`	Provides breakdown on how much memory a process is using so you can see how much is shared and how much is private. (Located in `/user/proc/bin`.)
`proctool`	Monitors processes and threads. (Available from Sun's web site.)
`snoop`	Monitors network traffic; indispensable when debugging low-level packets.
SymbEL/Virtual Adrian	A very powerful system monitoring toolkit. Provides the functionality of the above listed tools and more. Can be used to tune the `ncsize` and `ufs_ninod`e parameters and even has a mode to tune the operating system automatically.
`truss`	Provides information about which system calls a process makes.

Table 10.6 System Monitoring Tools - HP-UX

Tool	Description
`glance`	Provides detailed system information about open file descriptors, locks, threads, and so on.
`gpm`	Provides detailed system information about open file descriptors, locks, threads, and so on.
`tusc`	A system call trapper. Might not be available on all systems.
`sysdef`	Provides information about kernel parameters.
`landiag`	A tool for monitoring network statistics.
`sam`	System Administration Manager. A tool for general system administration.

Table 10.7 System Monitoring Tools - SGI Irix

Tool	Description
`dkstat`	Similar to `iostat`. Provides information about disk I/O and CPU use.
`gmemusage` (Irix 6.x)	X windows tool for viewing information about virtual memory.
`netstat -C`	Provides real-time, full-screen data.
`osview`	Provides full-screen information; combines functionality of `vmstat`, `mpstat`, and `netstat`.
`par`	Similar to `truss` on Solaris. Provides information about system calls made by a process.
Performance Copilot	An SGI add-in package.

Using SNMP

Netscape Messaging Server 4.0 supports the Simple Network Management Protocol (SNMP), version 1, and provides controls for configuring its SNMP subagent. Using SNMP and network management software, such as HP OpenView, you can monitor Messaging Server in real time as you do any other network device.

Under SNMP, data travels between a managed device and a network management station (NMS). A managed device is any device that runs SNMP; a server is a managed device. From the network management station, you can monitor the network remotely and exchange data between servers about network activity.

In Messaging Server, SNMP uses two agents to transfer information between the network management station and the managed device, the master agent and the subagent.

- The master agent handles all communication between servers, through their subagents, and the network management station. The master agent is installed with the Administration Server, and is controlled through its user interface. For more information, see *Managing Servers with Netscape Console*.
- The subagent for each server has access to its network information, which the subagent sends to the master agent when requested. The Messaging Server subagent is installed with Messaging Server and is controlled by the SMTP Settings form. For more information, see The Messaging Server Subagent.

Each server stores network information in the form of variables, or managed objects, which the network management station can query. The definitions for the server's managed objects are stored in the Management Information Base (MIB). For information about the Messaging Server MIB, see Appendix D, SNMP MIB.

Note: For more information about SNMP capabilities in Netscape Server products, see *Managing Servers with Netscape Console*.

For detailed information about the SNMP protocol, see RFC 1155 and RFC 1157.

Communication Between the NMS and the Managed Device

To exchange network information, SNMP uses protocol data units (PDUs), which contain information about the variables stored on the server. The network management station (NMS) and the server, or managed device, exchange PDUs in either of two ways:

- In network management station-initiated communication, the management station queries the server for data. This accounts for most communication between the management station and a server. Messaging Server 4.0 supports querying server data only.

  In a network management station-initiated session, the management station identifies which servers and variables to monitor by examining the MIB. Then, the management station sends a PDU to the master agent, which passes it to the subagent of the server. The subagent returns the data to the master agent, which sends it back in PDU form to the management station.

- In managed-device-initiated communication, SNMP uses traps to send information about network events, such as shutdown and startup.

  In a managed-device-initiated session, when a monitored event occurs, the subagent sends a trap to the master agent, which forwards it to the network management station. For information about traps, see MIB Traps in Appendix D, SNMP MIB.

Note: To send SNMP traps to the network management station, you must set the correct community and trap destination through the Administration Server. For more information, see *Managing Servers with Netscape Console*.

The Messaging Server Subagent

The Messaging Server's SNMP subagent, called `ns-mailagt`, gathers data about Messaging Server's network activity. You can configure some parts of the subagent through the SNMP Tab.

Before you can enable the Messaging Server subagent, you must start the master agent through the Administration Server user interface. The master agent handles communication between servers, through their subagents, and the

network management station. The subagents of all installed Netscape servers communicate with the same master agent. For information about the master agent, see *Managing Servers with Netscape Console*.

Once the master agent is available, you can start the subagent. The subagent does several things:

- It reads its configuration information, which is stored in Directory Server. This is the information you can set using the SNMP Tab.
- It initializes the Messaging Server MIB, which contains variables that store network information.
- It informs the master agent about the part of the MIB subtree that it monitors, and therefore what information it can provide. In this case, the Messaging Server subagent monitors, and can provide, only Messaging Server MIB data.

When the network management station sends a query, the master agent sends the request to the subagent through the SNMP Multiplexing (SMUX) protocol. The subagent queries the variables in the MIB and reports back to the master agent.

Periodically, the subagent checks the status of the Messaging Server. If it detects that the server has shut down, restarted, or failed to respond, it sends a trap to the network management station through the master agent. When the Administration Server terminates the subagent, the master agent unregisters the MIB, while the subagent performs any cleanup or logging and then exits.

For information about the Messaging Server MIB, see Appendix D, SNMP MIB. For information about the SMUX protocol, see RFC 1227.

SNMP Tab

You use the Messaging Server SNMP Settings form, which is part of Netscape Console, to set some options for the subagent, enable server statistics collection, and start or stop the subagent. After you modify the subagent, you must restart it before your changes can take effect.

To view and configure information subagent options, go to the SNMP Settings form.

1. In the Messaging Server Console, select the server for which you are setting subagent options.
2. Under Server Group, double-click the Configuration tab.
3. In the window on the right side of the page, click the SNMP tab.

   You see the SNMP Settings form.

Using this form, you can perform the following tasks:

- Configuring the Subagent
- Starting and Stopping the Subagent

To verify the changes you make using the SNMP Settings form, see Verifying SNMP Configuration Changes.

Configuring the Subagent

To configure the SNMP subagent on your system and enable statistics reporting to the network management station, you use the SNMP Settings form, which is part of Netscape Console.

Note: Before you can modify the subagent, the Messaging Server installation you want to configure and the master agent must be running. The master agent is enabled through the Administration Server's SNMP Master Agent Control form. For more information, see *Managing Servers with Netscape Console*.

Follow these steps to configure the subagent.

1. Go to the SNMP Settings form. For directions, see SNMP Tab.
2. At the top of the SNMP Settings form, configure the fields as follows:

   Master agent hostname. Use this field to enter the name of the host where the SNMP master agent resides. This must be a machine name, not an IP address. Default: `localhost`.

Master agent port number. Use this field to specify the port number the subagent uses to communicate with the master agent. Default: 199.

Organization name. Use this field to enter the name of the organization using Messaging Server. Usually this is a department or company name.

Server Description. Use this field to enter a text description that uniquely describes this Messaging Server installation, for example, the Messaging Server for Marketing.

Contact person info. Use this field to specify the person to contact about anything related to Messaging Server. Usually this is the server administrator. You can enter the name or email address of the contact, or both.

Server Location. Use this field to specify the location of this installation of Messaging Server. Usually this is a street address.

The information in these fields is stored in Netscape Directory Server for this installation.

3. Click Save.

   A message appears reminding you to restart the subagent so that the settings can take effect. *Before you can restart the subagent*, you must enable statistics collection.

4. Go on to Enabling Statistics Collection.

Enabling Statistics Collection

The subagent does not report SNMP statistics to the network management station unless you enable statistics collection on the SNMP Settings form, which is part of Netscape Console. If statistics collection is not enabled, the subagent cannot be started.

Important: If the network management station has problems getting Messaging Server's SNMP statistics, check the server log information, which is located in *`serverRoot`*`/mail-`*`instanceName`*`/log/default`, for information.

If the SNMP data collection process (`snmpcoll`), is not running, check the Administration Server Console to see whether the SNMP enable flag is on. In Messaging Server 3.x, this process starts when you start Messaging Server, whether SNMP is enabled or not. In Messaging Server 4.x, this flag applies to both the SNMP agent and `snmpcoll`. For more information, see *Managing Servers with Netscape Console*.

If you disable the startup server, this collection process is also disabled.

Follow these steps to enable data collection, after completing the steps in the section Configuring the Subagent.

1. Check the Enable Statistics Collection box.

   If you remove the check, the subagent cannot be enabled.

2. Restart the subagent by clicking the Start button.

   Your configuration information is stored in Directory Server, the subagent starts, and statistics collection begins.

3. If you want to verify your changes to this form, see Verifying SNMP Configuration Changes.

Starting and Stopping the Subagent

To start, stop, or restart the SNMP subagent, select one of three options at the bottom of the SNMP Settings form.

To start, stop, or restart the subagent:

1. Go to the SNMP Settings form. For directions, see SNMP Tab.

2. At the bottom of the form, click one of these buttons:

   Start. Messaging Server attempts to start the subagent.

   Stop. Messaging Server attempts to stop the subagent, if it is currently running.

   Restart. Messaging Server attempts to stop and then restart the subagent.

Note: If the SNMP subagent fails to start or stop, check the SNMP subagent log, which is located in *serverRoot*/mail-*instanceName*/log/default, for information.

Verifying SNMP Configuration Changes

You can verify the changes you make using the SNMP Settings form by entering a Messaging command in a command window.

Follow these steps to verify your changes to the subagent.

1. Open a Unix command window.
2. Go to the Messaging Server `bin` directory.
3. Enter the Messaging command `configutil`. For example:
   ```
   configutil | more
   ```

   You see all Messaging Server configuration statistics.
4. Scroll to the statistics whose names start with SNMP and find the settings you can configure using the SNMP Settings form:

   ```
   SNMP.master port | 199
   SNMP.contact
   SNMP.description
   SNMP.location
   ```

Chapter

11

Logging and Log Analysis

Netscape Messaging Server 4.0 can create log files that record events related to its administration, to communications using any of the protocols (IMAP, POP, and SMTP) that the server supports, and to other processes employed by the server. By examining the log files, you can monitor many aspects of the server's operation.

You can customize the policies for creating and managing the Messaging Server log files. This chapter describes the types and structure of log files, and discusses how to administer and how to view the log files.

This chapter has the following sections:

- Log Characteristics
- Defining Log Rotation, Expiration, and Backup Policies
- Searching and Viewing Logs
- Analyzing Logs with Third-Party Tools
- Selected Event-Message Formats
- Interface Reference: Logging and Log Files

Log Characteristics

Messaging Server logging is flexible and customizable. You can specify settings that affect which and how many events are logged, and you can use those settings and other characteristics to refine searches for logged events when you are analyzing log files.

Services That Are Logged

Messaging Server creates a separate set of log files for each of the major protocols, or services, it supports. You can customize and view each type of log file individually. Table 11.1 lists the services that can be logged.

Table 11.1 Logged Services

Service	Log-file description
Admin	Contains logged events related to communication between Netscape Console and Messaging Server (mostly through several CGI processes), by way of its Administration Server
SMTP	Contains logged events related to SMTP activity of this server
IMAP	Contains logged events related to IMAP4 activity of this server
POP	Contains logged events related to POP3 activity of this server
Default	Contains logged events related to other activity of this server, such as command-line utilities and other processes

Levels of Logging

The level, or priority, of logging defines how detailed, or verbose, the logging activity is to be. A higher priority level means less detail, because only events of high priority (high severity) are logged. A lower level means greater detail because more kinds of events are recorded in the log file.

You can set the logging level separately for each service (see Log Files Option Tab), and you can use logging level to filter searches for log events (see Log Viewer Window). Table 11.2 describes the available levels.

Table 11.2 Levels of Logging

Level	Description
Critical	The minimum logging detail. An event is written to the log whenever a severe problem or critical condition occurs--such as when the server cannot access a mailbox or a library needed for it to run.
Error	An event is written to the log whenever an error condition occurs--such as when a connection attempt to a client or another server fails.
Warning	An event is written to the log whenever a warning condition occurs--such as when the server cannot understand a communication sent to it by a client.
Notice	An event is written to the log whenever a notice (a normal but significant condition) occurs--such as when a user login fails or when a session closes.
Informational	An event is written to the log with every significant action that takes place--such as when a user successfully logs on or off or creates or renames a mailbox.
Debugging	The most verbose logging. Useful only for debugging purposes. Events are written to the log at individual steps within each process or task, to pinpoint problems.

Note: These Messaging-Server logging levels are a subset of those defined by the Unix `syslog` facility.

IMPORTANT: The more verbose the logging you specify, the more disk space your log files will occupy; for guidelines, see Defining Log Rotation, Expiration, and Backup Policies.

When you select a particular logging level, events corresponding to that level and to all higher (less verbose) levels are logged. The default level of logging is Notice.

Facility Categories

Within each supported service or protocol, Messaging Server further categorizes logged events by the facility, or functional area, in which they occur. Every logged event contains the name of the facility that generated it. These categories aid in filtering events during searches (see Log Viewer Window). Table 11.3 lists the facilities that Messaging Server recognizes for logging purposes.

Table 11.3 Facilities for log files

Facility	Description
General	Undifferentiated actions related to this protocol or service
LDAP	Actions related to Messaging Server accessing the LDAP directory database
Network	Actions related to network connections (socket errors fall into this category)
Account	Actions related to user accounts (user logins fall into this category)
Protocol	Protocol-level actions related to protocol-specific commands (errors returned by IMAP or POP functions fall into this category)
Stats	Actions related to the gathering of server statistics
Store	Low-level actions related to accessing the message store (read/write errors fall into this category)

See Searching and Viewing Logs for examples of using facility categories as filters in log searches.

Filename Conventions for Log Files

All log files created by Messaging Server use identical naming conventions. Each log file has a filename of the form

service.sequenceNum.timeStamp

where the components of the filename have these meanings:

service	The protocol or service being logged (see Table 11.1)
sequenceNum	An integer that specifies the order of creation of this log file compared to others in the log-file directory. Log files with higher sequence numbers are more recent than those with lower numbers. Sequence numbers do not roll over; they increase monotonically for the life of the server (beginning at server installation).
timeStamp	A large integer that specifies the date and time of file creation. (Its value is expressed in standard Unix time: the number of seconds since midnight January 1, 1970.)

For example, a log file named `imap.63.915107696` would be the 63rd log file created in the directory of IMAP log files, created at 12:34:56 PM on December 31, 1998.

The combination of open-ended sequence numbering with a timestamp gives you more flexibility in rotating, expiring, and selecting files for analyzing. See Defining Log Rotation, Expiration, and Backup Policies for more specific suggestions.

Content Format for Log Files

All log files created by Messaging Server have identical content formats. Log files are multiline text files, in which each line describes one logged event. All event descriptions, for each of the supported services, have the general format

dateTime hostName processName[*pid*]: *facility logLevel*: *eventMessage*

in which the components of the event description have these meanings:

dateTime	The date and time at which the event was logged, expressed in *dd/mon/yyyy hh:mm:ss* format, with a time-zone field expressed as *+/-hhmm* from GMT. For example: :02/Jan/1999:13:08:21 -0700
hostName	The name of the host machine on which the server is running: for example, showshoe. **Note:** If there is more than one instance of Messaging Server on the host, you can use the process ID component to separate logged events of one instance from another.
processName	The name of the process that generated the event: for example, cgi_store
pid	The process ID of the process that generated the event: for example, 18753
facility	The facility category that the event belongs to: for example, General (see Table 11.3)
logLevel	The level of logging that the event represents: for example, Notice (see Table 11.2)
eventMessage	An event-specific explanatory message that may be of any length: for example, Log created (894305624). For descriptions of the formats of some event messages, see Selected Event-Message Formats.

Note: This logging format is identical to the logging format defined by the Unix syslog facility, except that the date/time format is different and the format includes two additional components (*facility* and *logLevel*).

Here are three examples of logged events as viewed using Netscape Console (see Log Viewer Window).

```
02/May/1998:17:37:32 -0700 showshoe cgi_store[18753]: General Notice:
   Log created (894155852)

04/May/1998:11:07:44 -0400 xyzmail cgi_service[343]: General Error:
   function=getserverhello|port=2500|error=failed to connect

03/Dec/1998:06:54:32 +0200 AiriusPost imapd[232]: Account Notice:
   close [127.0.0.1] [unauthenticated] 1998/12/3 6:54:32 0:00:00 0 115 0
```

When viewing a log file in the Log Viewer window, you can limit the events displayed by searching for any specific component in an event, such as a specific logging level or facility, or a specific process ID. See Searching and Viewing Logs.

Log-File Directories

Every logged service is assigned a single directory, in which its log files are stored. All IMAP log files are stored together, as are all POP log files, and likewise for the other services. You define the location of each directory, and you also define how many log files of what maximum size are permitted to exist in the directory. (See Log Files Option Tab.)

Make sure that your storage capacity is sufficient for all your log files. Log data can be voluminous, especially at lower (more verbose) logging levels.

It is important also to define your logging level, log rotation, log expiration, and server-backup policies appropriately so that all of your log-file directories are backed up and none of them become overloaded; otherwise, you may lose information. See Defining Log Rotation, Expiration, and Backup Policies (next).

Defining Log Rotation, Expiration, and Backup Policies

You can define the logging configurations for Messaging Server that best serve your administration needs. This section discusses issues that may help you decide on the best configurations and policies, and it explains how to implement them.

Flexible Logging Architecture

The naming scheme for log files (*`service.sequenceNum.timeStamp`*) helps you to design a flexible log-rotation and backup policy. The fact that events for different services are written to different files makes it easier for you to isolate problems quickly. Also, because the sequence number in a filename is ever-increasing and the timestamp is always unique, later log files do not

simply overwrite earlier ones after a limited set of sequence numbers is exhausted. Instead, older log files are overwritten or deleted only when more flexible limits of age, number of files, or total storage are reached.

Messaging Server supports automatic rotation of log files, which simplifies administration and facilitates backups. You are not required to manually retire the current log file and create a new one to hold subsequent logged events. You can back up all but the current log file in a directory at any time, without stopping the server or manually notifying the server to start a new log file.

In setting up your logging policies, you can set options (for each service) that control limits on total log storage, maximum number of log files, individual file size, maximum file age, and rate of log-file rotation.

Setting Logging Options

You can use Netscape Console to set options that control the logging configuration for each Messaging Server service.

The optimal settings for these options depend on the rate at which log data accumulates. It may take between 4,000 and 10,000 log entries to occupy 1 MB of storage. At the more verbose levels of logging (such as Notice), a moderately busy server may generate hundreds of megabytes of log data per week. Here is one approach you can follow:

1. In Netscape Console, open the Messaging Server whose log file options you want to set.

2. Click the Configuration tab, open the Log Files folder in the left pane, and select the log files of a service (such as IMAP, SMTP, or Admin).

3. Click the Option tab in the right pane. The Option form for that logged service is displayed.

4. Pick a total storage limit that is within your hardware capacity and that coordinates with the backup schedule you have planned for the server. Estimate the rate at which you anticipate that log data will accumulate, add a factor of safety, and define your total storage limit so that it is not exceeded over the period between server backups.

Example: If you expect to accumulate an average of 3 MB of IMAP log-file data per day, and server backups are weekly, you might specify on the order of 25 - 30 MB as the storage limit for IMAP logs (assuming that your disk storage capacity is sufficient).

Put the value you choose into the "When total log size exceeds" field of the Log Files Option form.

5. Define your maximum number of log files, maximum age, and log-rotation schedule to coordinate with your backup schedule.

   Example: If server backups are weekly and you rotate IMAP log files daily, you might specify a maximum number of IMAP log files of about 10 (to account for faster rotation if the individual log-size limit is exceeded), and a maximum age of 7 or 8 days.

   Put the values you choose into the "Number of logs per directory", "When a log is older than", and "Create new log every" fields of the Log Files Option form.

6. Define your maximum log-file size so that searching performance is not impacted. Also, coordinate it with your rotation schedule and your total storage limit. Given the rate at which log entries accumulate, you might set a maximum that is slightly larger that what you expect to accumulate by the time a rotation automatically occurs. And your maximum file size times your maximum number of files might be roughly equivalent to your total storage limit.

   Example: If your IMAP log rotation is daily, your expected accumulation of IMAP log data is 3 MB per day, and your total storage limit for IMAP logs is 25 MB, you might set a maximum IMAP log-file size of 3.5 MB. (In this example, you could still lose some log data if it accumulated so rapidly that all log files hit maximum size and the maximum number of log files were reached.)

   Put the value you choose into the "File size for each log" field of the Log Files Option form.

7. For safety, pick a minimum amount free disk space that you will permit on the volume that holds the log files. That way, if factors other than log-file size cause the volume to fill up, old log files will be deleted before a failure occurs from attempting to write log data to a full disk.

   Put this value into the "When free disk space is less than" field of the Log Files Option form.

8. Assign a directory to hold your log files. Put this value into the "Directory path for log files" field of the Log Files Option form.

9. Set a level of logging that is consistent with your storage limits--that is, a level that you estimate will cause log-data accumulation at approximately the rate you used to estimate the storage limit. Put this value into the "Levels of detail" field of the Log Files Option form.

See Log Files Option Tab for a detailed description of the contents of that form.

Note that you must set several limits, more than one of which might cause the rotation or deletion of a log file. Whichever limit is reached first is the controlling one. For example, if your maximum log-file size is 3.5 MB, and you specify that a new log be created every day, you may actually get log files created faster than one per day if log data builds up faster than 3.5 MB every 24 hours. Then, if your maximum number of log files is 10 and your maximum age is 8 days, you may never reach the age limit on log files because the faster log rotation may mean that 10 files will have been created in less than 8 days.

The following default values, provided for Messaging Server administration logs, may be a reasonable starting point for planning:

maximum number of log files in directory: 10
maximum log-file size: 2 MB
total maximum size permitted for all log files: 20 MB
minimum free disk space permitted: 5 MB
log rollover time: 1 day
maximum age before expiration: 7 days
level of logging: Notice

You can see that this configuration assumes that server-administration log data is predicted to accumulate at about 2 MB per day, backups are weekly, and the total space allotted for storage of admin logs is at least 25 MB.(These settings may be insufficient if the logging level is more verbose.)

For SMTP, POP, or IMAP logs, the same values might be a reasonable start. If all services have approximately the same log-storage requirements as the defaults shown here, you might expect to initially plan for about 150 MB of total log-storage capacity. (Note that this is meant only as a general indication of storage requirements; your actual requirements may be significantly different.)

Searching and Viewing Logs

Netscape Console provides a basic interface for viewing Messaging Server log data. It allows for selecting individual log files and for performing flexible filtered searches of log entries within those files.

For a given service (such as SMTP), log files are listed in chronological order. Once you have chosen a log file to search, you can narrow the search for individual events by specifying a time interval, the logging level, facility category, and a text pattern for matching.

Search Parameters

These are the search parameters you can specify for viewing log data:

- You can specify the beginning and end of a specific time period to retrieve events from, or you can specify a number of days (before the present) to search. You might typically specify a range to look at logged events leading up to a server crash or other occurrence whose time you know of. Alternatively, you might specify a day range to look at only today's events in the current log file.
- You can specify the logging level (see Levels of Logging). You might select a specific level to uncover a specific problem; for example, Critical to see why the server went down, or Error to locate failed protocol calls.
- You can specify the facility (see Facility Categories). You might select a specific facility if you know the functional area that contains the problem; for example, Store if you believe a server crash involved a disk error, or Protocol if the problem lies in an IMAP protocol command error.

  Examples of combining logging level and facility in viewing logs might include

  - specifying Account facility (and Notice level) to display failed logins, which may be useful when investigating potential security breaches
  - specifying Network facility (and all logging levels) to investigate connection problems

- specifying all facilities (and Critical logging level) to look for basic problems in the functioning of the server

- You can provide a text search pattern to further narrow the search. You can include any component of the event (see Content Format for Log Files) that can be expressed in a wildcard-type search, such as event time, process name, process ID, and any part of the event message (such as remote hostname, function name, error number, and so on) that you know defines the event or events you want to retrieve.

  Your search pattern can include the following special and wildcard characters:

  `*` Any set of characters (example: `*.com`)
  `?` Any single character (example: `199?`)
  `[`*`nnn`*`]` Any character in the set *nnn* (example: `[aeiou]`)
  `[^`*`nnn`*`]` Any character not in the set *nnn* (example: `[^aeiou]`)
  `[`*`n-m`*`]` Any character in the range *n-m* (example: `[A-Z]`)
  `[^`*`n-m`*`]` Any character not in the range *n-m* (example: `[^0-9]`)
  `\` Escape character: place before `*`, `?`, `[`, or `]` to use them as literals

  Note: Searches are case-sensitive.

Specifying a Search and Viewing Results

Follow these steps to search for logged events with specific characteristics belonging to a given service:

1. In Netscape Console, open the Messaging Server whose log files you want to inspect.

2. Follow either of these steps to display the Log Files Content form for a given logged service:

   - Click the Tasks tab, then click "View *service* logs", where *service* is the name of the logged service (such as "IMAP service", "SMTP service", or "administration").

   - Click the Configuration tab, then open the Log Files folder in the left pane and select the log files of a service (such as IMAP, SMTP, or Admin). Then click the Content tab in the right pane.

3. The Content form for that logged service is displayed.
4. In the Log filename field, select the log file you want to examine.

   (See Log Files Content Tab for a detailed description of the contents of that form.)
5. Click the View selected log button to open the Log Viewer window.
6. In the Log Viewer window, specify your desired search parameters (described the next section, Search Parameters).
7. Click Update to perform the search and display the results in the Log entry field.

See Log Viewer Window for a detailed description of the contents of that window.

Analyzing Logs with Third-Party Tools

For log analyses and report generation beyond the display capabilities of Netscape Console, you need to use other tools. You can manipulate log files on your own with text editors, and you may also be able to modify and use existing report-generation tools that were developed to manipulate Unix `syslog` files.

With a scriptable text editor supporting regular-expression parsing, you can potentially search for and extract log entries based on any of the criteria discussed in this chapter, and possibly sort the results or even generate sums or other statistics.

If you wish to use a public-domain `syslog` manipulation tool, remember that you may need to modify it to account for the different date/time format and for the two extra components (*`facility`* and *`logLevel`*) that appear in Messaging Server log entries but not in `syslog` entries.

Selected Event-Message Formats

The event message of each log entry is in a format specific to the type of event being logged: that is, each service defines what content appears in any of its event messages. Many event messages are simple and self-evident; others are more complex.

To help you search for and interpret common log entries related to message transfer, this section describes the format of logged events written by three modules of the SMTP service: SMTP-Accept, SMTP-Deliver, and Mailbox-Deliver.

Note that the log-entry elements described here are all parts of the *eventMessage* portion of the log entry, where the entire entry has the format

dateTime hostName processName[*pid*]: *facility logLevel*: *eventMessage*

. See Content Format for Log Files for descriptions of the other portions.

SMTP-Accept log format

The event message for an SMTP-Accept log entry has the format

moduleName:*envelopeID*:*mailFrom*:[*peerAddr*ess]:*peerHost*:*msgID*:*msgSize*:
numRecipients:*recipientList*

Where the elements of the event message have the following meanings:

moduleName	The name of the SMTP module that logged the event (SMTP-Accept)
envelopeID	The ID assigned to the message by Messaging Server (unique to each received message)
mailFrom	The sender's address, from the message envelope
peerAddress	The IP address of the connecting server
peerHost	The host name (or IP address, if no lookup is performed) of the connecting server
msgID	The ID of the message, written by the sending client into the message header
msgSize	The size of the message, in bytes

numRecipients	The number of recipients
recipientList	The address of each recipient

Here is an example:

```
[08/Sep/1998:19:04:24 -0700] dizzy smtpd[8379]: General Notice:
   SMTP-Accept:0EYZV320.6U1:<aswe32dasdf@netscape.com>:[127.0.0.1]:
   127.0.0.1:<pkeni@netscape.com>:272:1:<dizzy2@dizzy.mcom.com>
```

SMTP-Deliver log format

The event message for an SMTP-Deliver log entry has the format

moduleName:*envelopeID*:*mailFrom*:*status*:*destHost*:*msgID*:*msgSize*:
numRecipients:*recipientList*

in which the elements of the event message have the following meanings:

moduleName	The name of the SMTP module that logged the event (`SMTP-Deliver`)
envelopeID	The ID assigned to the message by Messaging Server (unique to each received message)
mailFrom	The sender's address, from the message envelope
status	The delivery status of the message (`Delivered` or `Deferred`)
destHost	The host name of the destination server
msgID	The ID of the message, written by the sending client into the message header
msgSize	The size of the message, in bytes
numRecipients	The number of recipients
recipientList	The address of each recipient

Here is an example:

```
[08/Sep/1998:19:04:02 -0700] dizzy smtpd[8379]: General Notice:
   SMTP-Deliver:0EYZV2Q0.8C0:<aasdfasdfds@netscape.com>:Delivered:
   c3po.netscape.com:<pkeni@netscape.com>:337:1:<pkeni@netscape.com>
```

Mailbox-Deliver log format

The event message for a Mailbox-Deliver log entry has the format

moduleName:*envelopeID*:*msgSize*:*msgID*:*userID*

Where the elements of the event message have the following meanings:

moduleName	The name of the SMTP module that logged the event (`Mailbox-Deliver`)
envelopeID	The ID assigned to the message by Messaging Server (unique to each received message)
msgSize	The size of the message, in bytes
msgID	The ID of the message, written by the sending client into the message header
userID	The account name of the recipient to whom the message was delivered

Here is an example:

```
[31/Jul/1998:16:50:56 -0700] slug smtpd[19530]: General Notice:
   Mailbox-Deliver:0EWZGWV0.02Z:17943:<12345678.123@nowhere>:slug464
```

Interface Reference: Logging and Log Files

This section describes the Netscape Console interface elements that allow you to set logging options and view logs. See *Managing Servers With Netscape Console* for information on using Netscape Console to manage Messaging Server and other servers.

Log Files Option Tab

You use the form accessed through this tab to set logging characteristics for each type of service that Messaging Server logs.

For more information, see also Defining Log Rotation, Expiration, and Backup Policies.

The Option form has these elements:

Levels of detail. Use this menu to select the level of detail (verbosity) you want for this service's logging, in terms of what events are to be logged. These are the available levels:

Critical	Critical conditions are logged
Error	Error conditions are logged
Warning	Warning conditions are logged
Notice	Notices are logged
Informational	All significant actions are logged
Debugging	The most verbose logging (for debugging only)

When you select a specific level, events for that level and for all less verbose levels are logged. The default level of logging is Notice. For more information on logging levels, see Levels of Logging.

Directory path for log files. In this field, enter the location at which log files for this service are to be kept. Default is *instanceDirectory*/log/*service*, where *instanceDirectory* is the directory in which the files for this instance of Messaging Server reside.

> **Note:** Log data can be voluminous. Choose a directory that has adequate disk storage space and in which your log files will not overwhelm other files.

Log File Rotation Policy

File size for each log. In this field, specify the maximum size (in KB or MB) permitted for a log file of this type. When the file currently being written to exceeds that size, subsequent events are written into a new file, named according to the conventions are described in Filename Conventions for Log Files.

Create new log every. In this field, specify the maximum age (in hours or days) permitted for the log file currently being written to.When the current log file exceeds that age, subsequent events are written into a new file, named according to the conventions are described in Filename Conventions for Log Files.

> **IMPORTANT:** If you do not want to lose log data, make sure you adjust your log-rotation parameters and backup schedule (see Defining Log Rotation, Expiration, and Backup Policies) so that files are not deleted before they have been backed up.

Log File Expiration policy

Number of logs per directory. In this field, specify the maximum number of log files permitted in the directory specified in the Directory path for log files field. When this number of files is exceeded, the oldest log file in the directory is deleted.

When total log size exceeds. In this field, specify the maximum size (in KB or MB) permitted for the sum of all log files of this service. When this maximum is exceeded, the oldest log file in the directory is deleted.

When free disk space is less than. In this field, specify the minimum free disk space (in KB or MB) permitted on the storage volume to which the log files are written. If this minimum is surpassed, the oldest log file in the directory is deleted.

When a log is older than. In this field, specify the maximum age (in hours or days) permitted for any log file. When a file exceeds that age, it is deleted.

> **IMPORTANT:** If you do not want to lose log data, make sure you adjust your log-expiration parameters and backup schedule (see Defining Log Rotation, Expiration, and Backup Policies) so that files are not deleted before they have been backed up.

Action Buttons

Save. Click this button to commit any settings you have made in the Log Files Option form.

Reset. Click this button to return the form to the settings it displayed when you opened it (unless you have previously clicked Save, in which case the form returns the settings it had when you last clicked Save).

Help. Click this button to display online help (this document) describing the Log Files Option form.

Log Files Content Tab

You use the form accessed through this tab to view and search the contents of a given service's log files.

For more information, see also Searching and Viewing Logs.

The Content form has these elements:

Log file info. This table displays the following characteristics of the log file currently selected in the Log filename list: file type, file size, number of lines, date and time last modified.

Log filename. This list displays the names of all log files for this service. Select a log file in the list to display its characteristics or view its content. Log-file naming conventions are described in Filename Conventions for Log Files. Note that the current log file (the one being written to) has no numerical suffixes in its name.

View selected log. Click this button to open the Log Viewer (see Log Viewer Window), a window that allows you to search and view selected contents of the log file currently selected in the Log filename list.

Action Buttons

Help. Click this button to display online help (this document) describing the Log Files Content form.

Log Viewer Window

You use this window to configure searches on the contents of any Messaging Server log file, and to display the results of those searches.

For more information, see also Searching and Viewing Logs.

The Log Viewer window has these elements:

Filter

Specify time period. Click this radio button to enter a starting and ending date and time for searching. If the button is selected, only events that occurred between the times you specify in the From and To fields are displayed.

From. In this field, enter the start of the period for filtering log events. Enter a slash-separated date followed by a space and a colon-separated time (format = *yyyy/mm/dd hh:mm:ss*). This field applies only if the "Specify time period" radio button is selected.

To. In this field, enter the end of the period for filtering log events. Enter a slash-separated date followed by a space and a colon-separated time (format = *yyyy/mm/dd hh:mm:ss*). This field applies only if the "Specify time period" radio button is selected.

For the past *n* Day(s). Click this radio button to specify a number of days, rather than a starting and ending date and time, for filtering log events. If this radio button is selected, you can enter an integer number in the field, in which case all log events since that number of days before the present day will be displayed.

Facility. Use this menu to specify that only log events of a specific server facility, or functional area (such as General, LDAP, or Network), are to be displayed. (Logged facilities are described in Facility Categories.) You can select a single facility or all facilities.

Levels of detail. Use this menu to specify that only log events of a given level (such as Critical, Error, or Notice) are to be displayed. (Logging levels are described in Levels of Logging). You can select all levels or a single level; if you select a single level, events at that and all higher (less verbose) levels are included in the display.

Pattern. Use this field to enter a text pattern and specify that only log events that contain a match to that pattern are to be displayed. You can use these wildcard and special characters in the search pattern:

`*` Any set of characters (example: `*.com`)
`?` Any single character (example: `199?`)
`[`*nnn*`]` Any character in the set *nnn* (example: `[aeiou]`)
`[^`*nnn*`]` Any character not in the set *nnn* (example: `[^aeiou]`)

`[n-m]` Any character in the range *n-m* (example: `[A-Z]`)
`[^n-m]` Any character not in the range *n-m* (example: `[^0-9]`)
\ Escape character: place before `*`, `?`, `[`, or `]` to use them as literals

Note: Searches are case-sensitive.

Update. Click this button to apply the currently entered filter criteria to the specified log file. Events that match the criteria are displayed in the Log entry field.

Log Entry

Log entry. This field displays (in two panes) logged events from the current log file. (The file whose contents are displayed here has been selected through the Content form for a specific logged service; see Log Files Content Tab.)

Only entries that match the filter criteria specified by the other fields in this window are displayed. Each logged event occupies one line in the upper pane of the field and has the following format:

dateTime hostName processName[*pid*]: *facility logLevel*: *eventMessage*

For more information on log-entry format, see Content Format for Log Files.

Entries in the upper pane of the Log entry field may be truncated by the right edge of the field. However, the full text of any entry selected in the upper pane is displayed in the lower pane, wrapped to the width of the window.

Action Buttons

Close. Click this button to close the Log Viewer window.

Help. Click this button to display online help (this document) describing the Log Viewer window.

Appendix

A

Command-line Utilities

Netscape Messaging Server 4.0 provides a set of command-line utilities in addition to its graphical user interface. This appendix describes utilities for Messaging Server installation, migration, starting, stopping, administration, message management, problem recovery, monitoring, and reporting.

Each command-line utility has a set of options. Please note that these options might change in future releases as product functionality evolves.

This appendix includes the following sections:

- Overview of Command-Line Utilities
- Command-Line Utilities—General Information
- Messaging Server Utilities—Descriptions
- Alarm Attributes

There is a separate set of utilities used to migrate from a Unix `sendmail` messaging environment to Netscape Messaging Server 4.0. The `sendmail` utilities are described in Appendix C. The Messaging Server Mail Multiplexor and Mailstone components also have their own set of utilities. Although these additional utilities are summarized in this appendix, complete syntax and usage guidelines are found with the description of that component or process.

Overview of Command-Line Utilities

This overview briefly describes all of the Netscape Messaging Server 4.0 command-line utilities. This section contains five tables:

- Table A.1 groups the installation, message management, problem recovery, monitoring, and reporting utilities into categories according to their function and purpose.
- Table A.2 describes the installation, message management, problem recovery, monitoring, and reporting utilities in alphabetical order. For complete information about each utility, see Messaging Server Utilities—Descriptions.
- Table A.3 describes the `sendmail` migration utilities. For complete information on these utilities, see Appendix C.
- Table A.4 describes the Mail Multiplexor utilities. For complete information on these utilities, see the Mail Multiplexor document.
- Table A.5 describes the Mailstone utility programs. For complete information on these utilities, see the Mailstone document.

Table A.1 Command-line utilities by category

Category	Command-line Utilities
Installation and migration	`MoveUser, qconvert, upgrade`
Management	`configutil, imscripter, mboxutil, NscpMsg, processq`
Recovery	`deliver, reconstruct`
Background and daily tasks	`stored`
Monitoring and reporting	`counterutil, hashdir, mailq, quota, readership`

Table A.2 Command-line utilities and what they do

Command	What it does
`configutil`	Displays and makes changes to configuration information stored in the Directory Server or local configuration file.
`counterutil`	Displays all counters in a counter object. Monitors a counter object.
`deliver`	Delivers mail to a message store accessible by IMAP or POP.
`hashdir`	Identifies the directory that contains the message store for a particular user.
`imscripter`	The IMAP server protocol scripting tool. Executes a command or sequence of commands.
`mailq`	Checks the mail queue and reports the number of messages awaiting delivery.
`mboxutil`	Lists, creates, deletes, renames, or moves mailboxes.
`MoveUser`	Moves messages in a user's mailbox from one Messaging Server to another.
`NscpMsg` (Unix)	Starts and stops Messaging Server and runs recovery utilities.
`processq`	Manually delivers queued messages from the mail queue.
`qconvert`	Converts the Netscape Messaging Server 3.x message queue to the 4.0 format.
`quota`	Reports quota usage.
`readership`	Collects readership information on mailboxes.
`reconstruct`	Reconstructs mailboxes that have been damaged or corrupted.
`stored`	Performs background and daily tasks, expunges, and erases messages stored on disk.
`upgrade`	Converts Messaging Server mailboxes stored in 3.x format on a 3.x server to mailboxes in 4.0 format on a 4.0 server.

Table A.3 sendmail migration command-line utilities

Command	What it does
`chkuniq`	Checks the output files of the `unix2ldif` and `ldifsplit` utilities for duplicate entries. See Running the chkuniq Utility for details.
`ldapmodify`	Writes the contents of the converted, split, and checked LDIF files to the LDAP Directory. See Updating the LDAP Directory with ldapmodify for details.
`ldifsplit`	Takes the file of LDAP entries created by the `unix2ldif` utility and splits those entries into two groups: 1) LDAP entries that are already in the directory server (the DN already exists), and 2) LDAP entries that are not already in the directory server (no DN exists). See Running the ldifsplit Utility for details.
`MigrateUnixSpool`	Moves user messages from the user's `sendmail` spool file to the Messaging Server mailbox directory. See Running the MigrateUnixSpool Utility for details.
`unix2ldif`	Writes Unix `sendmail` user account data to an LDIF format file. See Running the unix2ldif Utility for details.

Table A.4 Mail Multiplexor utility programs

Command	What it does
`mmp-setup` (Unix)	Configures the Multiplexor for IMAP and POP services.
`PopProxy` (Unix) `PopProxy.exe` (NT)	The executable Multiplexor programs for POP services.
`ImapProxy` (Unix) `ImapProxy.exe` (NT)	The executable Multiplexor programs for IMAP services.
`ImapMMP` (Unix) `PopMMP` (Unix)	Shell scripts that set environment variables and execute Multiplexor for IMAP and POP services, respectively.

Table A.5 Mailstone utility programs

Program	What it does
`mailclient` (Unix) `mailclient.exe` (NT)	The principal Mailstone program—the one that talks to the mail server.
`mailmaster` (Unix)	The PERL script used to start all the `mailclient` instances and collect results.
`create_accounts_ldif` `create_broadcast_ldif`	Script tools used to create test mail accounts.
`loadclient` (Unix)	A shell script that facilitates directly running the `mailclient` program.

Command-Line Utilities—General Information

This section provides general information about using Netscape Messaging Server 4.0 command-line utilities.

Tip: A note about internationalization: If these utilities do not work correctly in your native environment, check the setting of the LANG environment variable.

Messaging Server File Locations

Messaging Server files are located in the following locations:

Table A.6 Command-line utilities location

Location	Utilities
server-root/bin/msg/admin/bin	configutil, counterutil, hashdir, imscripter, mboxutil, MoveUser, qconvert, quota, readership, reconstruct, upgrade
server-root/bin/msg/store/bin	deliver, stored
/etc	NscpMsg

Location of Configuration Data

All user and group configuration information is stored on the LDAP Directory Server.

Most Messaging Server configuration data is also stored on the LDAP server. Some Messaging Server configuration information is stored in a local file named `configdb` on the Messaging Server. The `configdb` file contains the following kinds of configuration information:

- Start up (bootstrap) information needed to locate the configuration data on the LDAP Directory Server
- Host and server names and types.
- Directory locations.
- Installation information. For example, in Unix environments the UID and GID the server is run as.

The `configdb` file is located:

- **Windows NT environments:** Messaging Server looks for the local `configdb` file in the directory specified in the registry. By default, that directory is *`server-root`*`\msg-`*`instance`*`\config`.
- **Unix environments:** Messaging Server looks for the local `configdb` file in the directory specified by the `CONFIGROOT` environment variable.

Usage Requirements

Most of the command-line utilities must be run locally on the messaging server. See the description of each utility for exceptions and command-specific login requirements.

Unix Login Requirements

In Unix environments, command-line utilities can only be run as `root` or as the login ID originally specified at the time of installation. By default, that is the `mailsrv` login ID. In other words, you have to log in as `mailsrv` to run these utilities.

Windows NT Login Requirements

In Windows NT environments, the default is that command-line utilities are run from the same account that is used to run services. By default, that is the Administrator account. Therefore, you must have administrator privileges to run most of the command-line utilities.

Messaging Server Utilities—Descriptions

This section describes what the main Netscape Messaging Server 4.0 command-line utilities do, defines their syntax, and gives examples of how they are used. The utilities are listed in alphabetical order.

configutil

The `configutil` utility enables you to list and change Messaging Server configuration options.

Most Messaging Server configuration options and values are stored in the LDAP database on the Directory Server with the remaining options and values stored locally on the Messaging Server in a file named `configdb` (see Location of Configuration Data for details).

configutil Syntax

`configutil [-f configdbfile] [command-options]`

Requirements: Must be run locally on the Messaging server.
Location: *server-root*/bin/msg/admin/bin

You can use `configutil` to perform four tasks:

- Display particular configuration options using `-o option`.
- List configuration option values using the `-e`, `-l`, or `-p prefix` options.
  - Use `-e` to include configuration options with empty values in the list.
  - Use `-l` to just list local configuration options from the server's local configuration file.
  - Use `-p prefix` to just list those configuration options whose names begin with the letters specified in *prefix*.
- Set configuration options using the `-o option` and `-v value` options.
  - Include the `-l` option with `-o option` and `-v value` to store the new value in the server's local configuration file.
  - To read the actual value from `stdin`, specify a dash (`-`) as the *value* on the command line.
- Import configuration option values from `stdin` using the `-i` option.
  - Include the `-e` option with the `-i` option to import configuration options even if the value of the configuration option is empty.
  - Include the `-l` option with the `-i` option to import all configuration options to the server's local configuration file.

Table A.7 configutil options

Option	Description
`-e`	Lists configuration options that do not have values specified. May be used with the `-l`, `-p`, and `-i` options.
`-f configdbfile`	Enables you to specify a local configuration file other than the default. (This option uses information stored in the CONFIGROOT environment variable by default.)

Table A.7 configutil options

Option	Description
`-i`	Imports configurations from standard input. Data to be entered in *`option`*`|`*`value`* format with no spaces on either side of the pipe. If you use `-e` with `-i`, and specify an option without a value, any existing value for that option is deleted. (If you do not use `-e`, when you specify an option without a value, no change is made to any existing value for that option.)
`-l` *`option`*	Lists configuration options stored in the local server configuration file. When used in conjunction with the `-v` option, specifies that an configuration option value be stored in the local server configuration file.
`-o` *`option`*	Specifies the name of the configuration option that you wish to view or modify. May be used with the `-l` and `-i` options. Configuration option names starting with the word `local` are stored in the local server configuration file.
`-p` *`prefix`*	Lists configuration options with the specified prefix.
`-v` *`value`*	Specifies a value for a configuration option. To be used with `-o` *`option`*. If the `-l` option is also specified or the configuration option name specified with the `-o` option begins with `local`, the option value is automatically stored in the local server configuration file rather than the Directory Server.

If you specify no command-line options, all configuration options are listed.

Examples of Ways to Use configutil

To list all configuration options and their values in the both the Directory Server LDAP database and local server configuration file:

```
configutil
```

To list all configuration options with the prefix `service.imap`:

```
configutil -p service.imap
```

To list all configuration option with the prefix `service.imap`, including those with empty values:

```
configutil -e -p service.imap
```

To display the value of the `service.smtp.port` configuration option:

```
configutil -o service.smtp.port
```

To set the value of the `service.smtp.port` configuration option to 25:

```
configutil -o service.smtp.port -v 25
```

To clear the value for the `service.imap.banner` configuration option:

```
configutil -o service.imap.banner -v ""
```

(See Alarm Attributes for information on using `configutil` to set alarm attributes.)

counterutil

The `counterutil` utility displays and changes counters in a counter object. It can also be used to monitor a counter object every 5 seconds.

counterutil Syntax

`counterutil -o` *`counterobject`* `[-r` *`registryname`*`]`

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.8 counterutil options

Option	Description
`-o` *`counterobject`*	Continuously display the contents of a particular counter object every 5 seconds.
`-r` *`registryname`*	Indicates the counter registry to use. If no counter is specified with the `-r` *`registryname`* option, the default is *`server-root`*`/msg-`*`instance`*`/counter/counter.`

Examples of Ways to Use counterutil

To list all counter objects in a given server's counter registry:

```
counterutil
```

To display the content of counter object `imapstat` every 5 seconds:

```
counterutil -o imapstat -r server-root/msg-instance/counter/counter
```

deliver

The `deliver` utility delivers mail directly to the message store accessible by IMAP or POP mail clients.

If you are administering an integrated messaging environment, you can use this utility to deliver mail from another MTA, a `sendmail` MTA for example, to the Messaging Server message store.

deliver Syntax

```
deliver [-l] [-d] [-r address] [-f address] [-m mailbox] [-a authid]
  [-q] [-F flag]...[userid]...
```

Requirements: Must be run locally on the Messaging server.
Location: *server-root*/bin/msg/store/bin

Table A.9 deliver options

Option	Description
-a *authid*	Specifies the authorization id of the sender. Defaults to anonymous.
-d	This option is recognized by `deliver` in order to maintain compatibility with `/bin/mail`, but it is ignored by `deliver`.
-F *flag*	Sets the system flag or keyword flag on the delivered message.
-f *address*	Inserts a forwarding path header containing *address*.
-l	Accepts messages using the LMTP protocol (RFC 2033).

Table A.9 deliver options

Option	Description
`-m` *`mailbox`*	Delivers mail to *`mailbox`*. • If any user ids are specified, attempts to deliver mail to *`mailbox`* for each user id. If the access control on a mailbox does not grant the sender the "`p`" right or if the `-m` option is not specified, then this option delivers mail to the inbox for the user ID, regardless of the access control on the inbox. • If no user ids are specified, this option attempts to deliver mail to *`mailbox`*. If the access control on a mailbox does not grant the sender the "`p`" right, the delivery fails.
`-q`	Overrides mailbox quotas. Delivers messages even when the receiving mailbox is over quota.
`-r` *`address`*	Inserts a `Return-Path:` header containing *`address`*.
`userid`	Deliver to inbox of the user specified by *`userid`*.

If you specify no options, mail is delivered to the inbox.

Examples of Ways to Use deliver

To deliver the contents of a file named `message.list` to Fred's Tasks mailbox:

```
deliver -m tasks fred < message.list
```

In this example, if the tasks mailbox does not grant "p" rights to the sender, the contents of `message.list` are delivered to the inbox of the user `fred`.

hashdir

The `hashdir` utility identifies the directory that contains the message store for a particular account. This utility reports the relative path to the message store, such as `d1/a7/`. The path is relative to the directory level just before the one based on the user ID. The utility sends the path information to the standard output.

hashdir Syntax

```
hashdir [-a] [-i] account_name
```

Requirements: Must be run locally on the Messaging server.
Location: *server-root*/bin/msg/admin/bin

Table A.10 hashdir options

Option	Description
-a	Appends the directory name to the output.
-i	Allows you to use the command in interactive mode.

imscripter

The `imscripter` utility connects to an IMAP server and executes a command or a sequence of commands.

imscripter Syntax

```
imscripter [-h] [-f script | [-c command] -f datafile]] [-c command]
  [-s serverid | -p port | -u userid | -x passwd |-v verbosity]
```

Requirements: May be run remotely.
Location: *server-root*/bin/msg/admin/bin

Table A.11 imscripter options

Option	Description
`-c` *`command`*	Executes *`command`*, which can be one of the following: create *`mailbox`* delete *`mailbox`* rename *`oldmailbox newmailbox`* [*`partition`*] getacl *`mailbox`* setacl *`mailbox userid rights`* deleteacl *`mailbox userid`* If one or more of the above variables are included, the option executes the given command with that input. For example, `create lincoln` creates a mailbox for the user `lincoln`. If the `-f` *`file`* option is used, the option executes the command on each variable listed in the file.
`-f` *`file`*	The *`file`* may contain one or more commands, or a list of mailboxes on which commands are to be executed.
`-h`	Displays help for this command.
`-p` *`port`*	Connects to the given port. The default is 143.
`-s` *`server`*	Connects to the given server. The default is `localhost`. The *`server`* can either a host name or an IP address.
`-u` *`userid`*	Connects as *`userid`*.

Table A.11 imscripter options

Option	Description
`-v` *`verbosity`*	String containing options for printing various information. The options are as follows. The default is `EPBibo` (`EBb` if `-f` is specified.) E - Show errors I - Show informational messages P - Show prompts C - Show input commands c - Show protocol commands B - Show BAD or NO untagged responses O - Show other untagged responses b - Show BAD or NO completion results o - Show OK completion results A - Show all of the above The letters designating options can be entered in any order.
`-x` *`passwd`*	Uses this password.

imscripter File Formats

Data files used with the `-f` option have to be formatted as a list of mailboxes with fully qualified paths, one mailbox per line. For example:

```
shared folders/indira/INBOX
shared folders/makeba/INBOX
shared folders/vladmir/INBOX
```

Scripts used with the `-f` option have to be in the following format:

```
command options
```

For example, an `imscripter` script file that adds the mailboxes contained in a file named `add.list`, and deletes mailboxes contained in a file named `delete.list`, looks like this:

```
create -f add.list
delete -f delete.list
```

Suppose the example file shown above is named `dothis.script`. To run it showing only errors, input commands, BAD and NO untagged and completion responses, enter:

```
imscripter -v ECBb -f dothis.script.
```

Examples of Ways to Use imscripter

To run `imscripter` in interactive mode:

```
imscripter [options]
```

In interactive mode, each command is entered one line at a time at the `imscripter` prompt. The command is then executed and responses displayed.

To execute the commands specified in a script file:

```
imscripter [options] -f script
```

To execute a specific command on *`mailbox`*:

```
imscripter [options] [-l] -c command mailbox
```

To execute a specific command for each line of data in a data file:

```
imscripter [options] -c command -f datafile
```

To execute commands from the specified script file:

```
imscripter -s username.airius.com -f script
```

mailq

The `mailq` utility checks and reports on the mail queue of messages awaiting delivery.

mailq Syntax

```
mailq [-v]
```

Requirements: Must be locally run on the server.
Location: `/bin/mailq`

Table A.12 mailq options

Option	Description
-v	Provides more verbose information about the queue.

mailq Examples

To check the mail queue, type `mailq` at a command prompt. If there are no queued messages, that fact will be reported:

```
% mailq
Mail queue is empty.
```

If there are queued messages, each host that has queued messages waiting to be delivered will be listed, along with the number of pending deliveries. For example, output might look like this:

```
% mailq
Queued Messages       Destination Host
---------------       ----------------
              2         math.marsu.edu
              3   universal-robots.com
```

In the example above, five messages are waiting for delivery. Delivering all of them should require two connections to other machines because the messaging server attempts to deliver all queued mail for a host before disconnecting.

See `processq` for information how to manually force immediate delivery of messages in the mail queue.

mboxutil

The `mboxutil` utility lists, creates, deletes, renames, or moves mailboxes (folders).

mboxutil Syntax

```
mboxutil [-c mailbox] [-d mailbox] [-r oldname newname [partition]]
  [-l] [-p pattern] [-x]
```

Requirements: Must be run locally on the Messaging server.
Location: *server-root*/bin/msg/admin/bin

Mailboxes are specified with names in the format *user/userid/sub-mailbox*. Where *userid* is the user that owns the mailbox. For example, the inbox of the user `desdemona` is entered as: `user/desdemona/INBOX`.

Table A.13 mboxutil options

Option	Description
`-c` *`mailbox`*	Creates the specified mailbox.
`-d` *`mailbox`*	Deletes the specified mailbox.
`-l`	Lists all of the mailboxes on a server.
`-p` *`pattern`*	When used in conjunction with the `-l` option, lists only those mailboxes with names that begin with the letters specified by *`pattern`*. You can use IMAP wildcards.
`-r` *`oldname newname`* [*`partition`*]	Renames the mailbox from *`oldname`* to *`newname`*. To move a folder from one partition to another, specify the new partition with the *`partition`* option.
`-x`	When used in conjunction with the `-l` option, shows the path and access control for a mailbox.

Examples of Ways to Use mboxutil

To list mailboxes:

```
mboxutil -l
```

To list all folders and also include path and `acl` information:

```
mboxutil -l -x
```

To create a mailbox named `INBOX` for the user `druscilla`:

```
mboxutil -c user/druscilla/INBOX
```

To delete a mailbox named `INBOX` for the user `delilah`:

```
mboxutil -d user/delilah/INBOX
```

To rename Daphne's mailbox from `memos` to `memos-april`:

```
mboxutil -r user/daphne/memos user/daphne/memos-april
```

MoveUser

The `MoveUser` utility moves a user's account from one mail server to another. When user accounts are moved from one mail server to another, it's also necessary to move the user's mailboxes and the messages they contain from one server to the other. In addition to moving mailboxes from one server to another, `MoveUser` updates entries in the Directory Server to reflect the user's new `mailhost` name and message store path.

MoveUser Syntax

```
MoveUser -s srcmailhost -x proxyuser -p password
  [-u uid] [-l ldapURL -D bindDN -w password] -d destmailhost [options]
```

Requirements: May be run remotely.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.14 MoveUser options

Option	Description
`-a` *`destproxyuser`*	ProxyAuth user for destination mail server.
`-A`	Do not add an alternate email address to the ldap entry.
`-d` *`destmailhost`*	Destination mail server.
`-D` *`binddn`*	Binding *`dn`* to the given *`ldapURL`*.
`-F`	Delete messages in source mail server after successful move of mailbox. (If not specified, messages will be left in source mail server.)
`-h`	Display help for this command.
`-l` *`ldapURL`*	URL to establish a connection with the Directory Server: `ldap://`*`hostname`*`:`*`port`*`/` *`base_dn`*`?`*`attributes`*`?`*`scope`*`?`*`filter`* For more information about specifying an LDAP URL, see your Directory Server documentation. Cannot be used with the `-u` option.
`-L`	Add a license for Messaging Server if not already set.

Table A.14 MoveUser options

Option	Description
`-m` *`destmaildrop`*	Message store path for destination mail server. (If not specified, the default is used.)
`-n` *`msgcount`*	Number of messages to be moved at once.
`-o` *`srcmaildrop`*	Message store path for source mail server. (If not specified, the default is used.)
`-p` *`srcproxypasswd`*	ProxyAuth password for source mail server.
`-s` *`srcmailhost`*	Source mail server.
`-S`	Do not set new message store path for each user.
`-u` *`uid`*	User ID for the user mailbox that is to be moved. Cannot be used with `-l` option.
`-v` *`destproxypwd`*	ProxyAuth password for destination mail server.
`-w` *`bindpasswd`*	Binding password for the *`binddn`* given in the `-D` option.
`-x` *`srcproxyuser`*	ProxyAuth user for source mail server.

Examples of Ways to Use MoveUser

To move all users from *`host1`* to *`host2`*, based on account information in the Directory Server `airius.com`:

```
MoveUser -l
  "ldap://airius.com:389/o=Airius.com???(objectclass=mailrecipient)"
  -D "cn=Directory Manager" -w password -s host1 -x admin -p password
  -d host2 -a admin -v password
```

To move one user from *`host1`* to *`host2`*, based on account information in the Directory Server `airius.com`:

```
MoveUser -l
  "ldap://airius.com:389/o=Airius.com???(uid=userid)"
  -D "cn=Directory Manager" -w password -s host1 -x admin
  -p password -d host2 -a admin -v password
```

To move a group of users whose uid starts with letter ‘s’ from `host1` to `host2`, based on account information in the Directory Server `server1.airius.com`:

```
MoveUser -l
  "ldap://server1.airius.com:389/o=Airius.com???(uid=s*)"
```

```
  -D "cn=Directory Manager" -w password -s host1 -x admin
  -p password -d host2 -a admin -v password
```

To move a user's mailboxes from *host1* to *host2* when the user ID is specified in the command line:

```
MoveUser -u
  uid -s host1 admin -p password
  -d host2 -x admin -v password -o /var/mail/spool/mailbox
  -m /usr/netscape/suitespot4/msg-airius/store/partition/primary
```

NscpMsg

The NscpMsg utility starts, stops, and refreshes the Messaging Server services. This utility is only available in Unix environments.

NscpMsg Syntax

```
/etc/NscpMsg start [imap | pop | smtp | store]
/etc/NscpMsg stop [imap | pop | smtp | store]
/etc/NscpMsg refresh [imap | pop | smtp | store]
```

Requirements: Must be run as root locally on the Messaging server.

Location: /etc
server-root/bin/msg/admin/bin

The NscpMsg utility sets the CONFIGROOT and LD_LIBRARY_PATH environment variables for the commands it runs.

NscpMsg is similar to the /etc/NscpMail utility supplied with Messaging Server 3.x.

Table A.15 NscpMsg options

Option	Description
refresh	Refresh mail server processes.
start	Starts all mail server processes (stored, smtpd, popd, imapd), or optionally, one specified service.
stop	Stops all mail server processes (stored, smtpd, popd, imapd), or optionally, one specified service.

processq

The `processq` utility immediately delivers messages in the deferred queue.

processq Syntax

`processq [[-R]`*`hostname`*`]`

Requirements: Must be locally run on the server.
Location: `/usr/lib`

Table A.16 processq options

Option	Description
`hostname`	Deliver mail addressed to *`hostname`*. The *`hostname`* can be the full name of the host as reported by `mailq`, or any pattern contained in the name. If the pattern matches more than one *`hostname`*, each match will have its queue processed.
`-R`	Specify a specific domain.

The deferred queue is automatically processed at regular intervals, so you normally never need to deliver the queue manually with the `processq` utility. You can also manage the queue by using the Netscape Console. For more information, see Managing the Message Queue in Chapter 3.

processq Examples

To deliver all messages in the deferred queue:

```
/usr/lib/processq
```

To deliver all queued mail addressed to `math.marsu.edu`:

```
/usr/lib/processq -Rmath.marsu.edu
```

To deliver all queued mail addressed to all hosts in the domain `marsu.edu`:

```
/usr/lib/processq '*.marsu.edu'
```

qconvert

The `qconvert` utility converts the Netscape Messaging Server 3.x message queue to the Netscape Messaging Server 4.0 format.

Examples of Ways to Use qconvert

`qconvert [-s sourceq -d targetq] [-l] [-r] [-h] [-f configdbfile]`

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.17 qconvert options

Option	Description
`-d targetq`	Specifies the pathname of the new message queue.
`-h`	Displays help for this command.
`-l`	Writes the results to the screen. If you do not specify this option, `qconvert` writes results to the default log file in the `log/default` directory.
`-r`	Removes messages after conversion.
`-s sourceq`	Specifies the pathname of the old message queue.
`-f configdbfile`	Specifies the pathname of the configuration database.

If you do not specify the location of the 3.x message queue or the 4.0 message queue, the `qconvert` utility reads the 3.x and 4.0 configuration files to locate the message queue directories. Consequently, if you do not specify the message queue locations, the following configuration information must be available to the `qconvert` utility.

For Messaging Server 3.x, configuration information is determined as shown in Table A.18:

Table A.18 Messaging Server 3.x configuration information

Unix	Windows NT
`MASTERCONFIG` environment variable `/etc/netscape.mail.conf`	Registry key in HKEY_LOCAL_MACHINE: `SOFTWARE\\Netscape\MessagingServer\\3.0`

For Messaging Server 4.0, configuration information is determined as shown in Table A.19 :

Table A.19 Messaging Server 4.0 configuration information

Unix	Windows NT
`CONFIGROOT` environment variable `/etc/nsserver.cfg`	Registry key in HKEY_LOCAL_MACHINE: `SOFTWARE\\Netscape\MessagingServer\\4.0`

The `qconvert` utility reads the 3.x directories in the following order: *`sourceq`*`/control`, *`sourceq`*`/deferred`, *`sourceq`*`/messages`. These directories are subdirectories of the post office directory that was specified at installation time.

The `qconvert` utility reads and converts the 3.x directories as follows:

1. The utility reads the 3.x control files and rewrites them into the 4.0 envelope log file located in *`targetq`*`/control/env-`*`date`*`-1`.
2. The utility reads the 3.x `deferred` directory and creates an envelope file for every subdirectory in the 4.0 `deferred` directory.
3. The utility merges the 3.x message header file (`-Header`) and message body file (`-Body`) into one 4.0 file located in *`targetq`*`/control/`*`msgname`*.

The utility automatically converts 3.x access rights to 4.0 access rights so that users have access to the appropriate files.

quota

The `quota` utility reports mailbox quota usage. This utility generates a report listing quotas, giving their limits and usage.

quota Syntax

`quota [user/`*`user-id`*`...]`

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.20 quota options

Option	Description
`user/`*`user-id`*	The quota listing is limited to quota roots with names that start with one of the given user IDs.

Netscape Messaging Server 4.0 supports quotas at the root (inbox) level. Quotas on subdirectories are not supported.

readership

The `readership` utility reports on how many users other than the mailbox owner have read messages in a shared mailbox. This utility scans all mailboxes.

A mailbox owner may grant permission for others to read mail in the owner's box. Administrators can use the `readership` utility to see how many users are accessing a mailbox other than the owner.

readership Syntax

`readership [-d `*`days`*`] [-p `*`months`*`]`

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.21 readership options

Option	Description
`-d` *`days`*	Counts as a reader any identity that has selected the mailbox within the indicated number of days. The default is 30.
`-p` *`months`*	Does not count users who have not selected the mailbox within the indicated number of months. The default is infinity and removes (prunes) the seen flag data for those users. This option also removes the "seen" flag data for those users from the store.

This utility produces one line of output per mailbox, reporting the number of readers followed by a space and the name of the mailbox.

Each reader is a distinct authentication identity that has selected the mailbox within the past specified number of days. Users are not counted as reading their own personal mailboxes. Personal mailboxes are not reported unless there is at least one reader other than the mailboxes owner.

reconstruct

The `reconstruct` utility rebuilds one or more mailboxes, or the master mailbox file, and repairs any inconsistencies. You can use this utility to recover from almost any form of data corruption in the mail store.

Note that low-level database repair, such as completing transactions and rolling back incomplete transactions is performed with `stored -d`.

reconstruct Syntax

`reconstruct [-p` *`partition`*`] [-r [`*`mailbox`*` [`*`mailbox...`*`]] | [-m] [-q]`

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Note: Netscape recommends that you shut down your server before running the `reconstruct` utility.

Table A.22 reconstruct options

Option	Description
`-m`	Performs a high-level consistency check and repair of the mailboxes database. This option assumes that `stored` is running. This option examines every mailbox it finds in the spool area, adding or removing entries from the mailboxes database as appropriate. The utility prints a message to the standard output file whenever it adds or removes an entry from the database.
`-p` *`partition`*	Specifies a partition name. You can use this option on the first usage of *`reconstruct`*.
`-q`	Fixes any inconsistencies in the quota subsystem, such as mailboxes with the wrong quota root or quota roots with the wrong quota usage reported.
`-r [`*`mailbox`*`]`	Performs a consistency check and repairs the partition area of the specified mailbox or mailboxes. The `-r` option also repairs all sub-mailboxes within the specified mailbox. If you specify `-r` with no mailbox argument, the utility repairs the spool areas of all mailboxes within the database.

The *`mailbox`* argument indicates the mailbox to be repaired. You can specify one or more mailboxes. Mailboxes are specified with names in the format *`user/userid/sub-mailbox`*. Where *`userid`* is the user that owns the mailbox. For example, the inbox of the user `dulcinea` is entered as: `user/dulcinea/INBOX`.

Examples of Ways to Use reconstruct

To rebuild all mailboxes in the `primary` partition:

```
reconstruct -r -p primary
```

To rebuild mailboxes listed in the command line argument only if they are in the `primary` partition:

```
reconstruct -p primary mbox1 mbox2 mbox3
```

To perform a high-level consistency check and repair of the mailboxes database:

```
reconstruct -m
```

You should use the `-m` option when:

- One or more directories were removed from the store spool area, so the mailbox database entries also need to be removed.
- One or more directories were restored to the store spool area, so the mailbox database entries also need to be added.
- The `stored -d` option is unable to make the database consistent.

If the `stored -d` option is unable to make the database consistent, you should:

1. Shut down all servers.
2. Remove all files in *`server-root`*`/msg-`*`instance`*`/store/mboxlist`.
3. Run `stored`.

   In Unix environments, start `stored` by entering:

   ```
   /etc/NscpMsg
   start store
   ```

4. Run `reconstruct -m` to build a new mailboxes database from the contents of the spool area.
5. After `reconstruct -m` completes, restart the server processes.

To rebuild the spool area for the mailboxes belonging to the user `crowe:`

```
reconstruct -r user/crowe
```

To rebuild the spool area for all mailboxes listed in the mailbox database:

```
reconstruct -r
```

You should use the `-r` option when:

- Accessing a mailbox returns one of the following errors: “System I/O error” or “Mailbox has an invalid format”.
- Accessing a mailbox causes the server to crash.
- Files have been added to or removed from the spool directory.

stored

The `stored` utility performs the following functions:

- background and daily messaging tasks
- low-level database consistency check and repair
- deadlock detection and rollback of deadlocked database transactions
- cleanup
- expiration, expunging, and erasing messages stored on disk
- alarm setting

The stored automatically performs cleanup and expiration operations once a day at midnight. You can choose to run additional cleanup and expiration operations.

How Messages are Deleted

Messaging Server messages are erased in three stages:

1. **Delete**. An IMAP or POP client marks the message to be deleted. IMAP clients mark messages with a `/deleted` flag, POP clients use the `DELE` command. This is referred to as *deleting* a message. At this point, the client can restore the message by removing the "deleted" marking.

2. **Expunge**. A client, or the expiration policies you have specified, expunges messages that have been marked deleted from the mailbox. (IMAP clients do this with the `EXPUNGE` command. POP clients expunge a mailbox with the `QUIT` command.) Once messages are expunged, the client can no longer restore them, but they are still stored on disk. (A second POP or IMAP client with an existing connection to the same mailbox may still be able to fetch the messages.)

3. **Cleanup**. The `stored` utility erases messages from the disk that have been expunged for at least one hour.

stored Syntax

To run `stored` from the command line to perform a specific operation:

```
stored [-1] [-c] [-n] [-h hour] [-v [-v]]
```

To run `stored` as daemon:

```
stored [-d] [-h hour] [-v [-v]]
```

Requirements: Must be run locally on the Messaging server.
Location: *`server-root`*`/bin/msg/admin/bin`

Table A.23 stored options

Option	Description
`-c`	Performs one cleanup pass to erase expunged messages. Runs once, then exits. The `-c` option is a one-time operation, so you do not need to specify the `-1` option.
`-d`	Run as daemon. Performs system checks and activates alarms, deadlock detection, and database repair.
`-h` *`hour`*	Run an additional cleanup and expiration operation. The *`hour`* value designates the hour of the day that `stored` is to automatically run. Specify *`hour`* in 24 hour format. For example `23` means 11pm. You do not need to use the `-1` option when using `-h`.
`-1`	Run once, then exit.
`-n`	Run in trial mode only. Does not actually expire or cleanup messages. Runs once, then exits.
`-v`	Verbose output.
`-v -v`	More verbose output.

Examples of Ways to Use stored

To test expiration policies:

```
stored -c
```

To perform a single cleanup pass:

```
stored -n -v
```

If you want to change the time of the automatic cleanup and expiration operations, use the `configutil` utility as follows:

```
configutil -o store.expirestart -v 21
```

upgrade

The `upgrade` utility transfers mailboxes stored in 3.x format on a 3.x server to Netscape Messaging Server 4.0 format mailboxes.

The `upgrade` utility is similar to the `migrate` utility provided by 3.x. The 3.x utility migrated both users and their mailboxes. The Messaging Server `upgrade` utility only transfers mailboxes since the way users are stored has not changed from 3.x to 4.0.

The 4.0 `upgrade` utility assumes that both Messaging Server 3.x and Messaging Server 4.0 reside on the same machine. The utility transfers the 3.x mailboxes on a machine to 4.0 format mailboxes on the same machine. Once `upgrade` has been run, you cannot start up the 3.x processes.

The 4.0 upgrade process occurs in two steps: (1) The folders are upgraded. (2) The messages are upgraded. You must update the folders (by using the `-s` option) before you update the messages (by using the `-m` or `-u` options). The message upgrade is a multi-threaded process. You can specify the number of threads by using the `-t` option.

The 4.0 `upgrade` utility first searches the LDAP server to find all the user mailboxes in that machine (users are considered to belong the 3.x server if their `mailhost` attribute is one of the `MessageHostNames` in that 3.x server). It then creates a one-to-one mailbox-mapping information in the 4.0 mailbox database. These mailboxes are marked as "`TRANSITION`".

Based on the options you specify, `upgrade` can transfer all 3.x mailboxes immediately. In NT environments, the `upgrade` utility retrieves the 3.x information through the registry. In Unix environments, the `upgrade` utility retrieves the 3.x information through a predefined configuration file. The `upgrade` does not change the 3.x directory structure, so 4.0 must be put in a different directory.

If you have 3.x mailboxes located in non-default mailbox paths, the `upgrade` utility tries to create a 4.0 mailbox directory in that mailbox path, and uses a number (such as `001`) to automatically assign the 4.0 partition name. In 4.0, the partition name is a logical name of a physical directory where user mailboxes can be physically created.

You can find the detailed mailboxes mapping information in the `upgrade.conf` file in the default 3.x mailbox directory.

If you want to save disk space, you can use the `-r` option to remove the messages after the upgrade.

If you have servers on multiple machines, you must run `upgrade` on each different machine.

Note: The 3.x mailboxes might require more disk space after the upgrade to 4.x. For more information on the upgrade process, see the server installation instructions.

upgrade Syntax

```
upgrade [-s] [-m] [-u userlist] [-i] [-r] [-h] [-f configdbfile]
   [-l ldapURL] [-t number]
```

Requirements: Must be run locally on the Messaging server.
Location: *server-root*/bin/msg/admin/bin

Table A.24 upgrade options

Option	Description
`-f` *configdbfile*	Identifies the file name of the *configdbfile* instance.
`-h`	Displays help for this command.
`-i`	Transfer the inbox first. Can be used only with the `-m` option.
`-l` *ldapURL*	Identifies the LDAP URL for the 3.x directory server in which user and group information is stored.
`-m`	Transfers the mailboxes immediately. You must create mailbox mapping with the `-s` option before using -m for the first time. For example, `-s -m`. This can be used in a script.
`-r`	Remove messages after transfer.
`-s`	Creates the one-to-one mailbox mapping, but delays transfer. This can be used in a script. You must run the `-s` option before you run the `-m` option or the `-u` option.
`-t` *number*	Specifies how many threads to start up for upgrading mailboxes. The default number is 25 threads.
`-u` *userlist*	Transfers all mail folders belonging to the user or users in specified in *userlist*.

Alarm Attributes

Alarm attributes specify how often system checks and other monitoring functions are performed. When a problem is detected an alarm message is sent to the specified person. (System checks are performed by the `stored` utility.)

You can modify the following alarm attributes by using the `configutil` command.

Table A.25 Email Alarm Attributes

Email Attributes	Default Value
`alarm.msgalarmnoticehost`	localhost
`alarm.msgalarmnoticeport`	25
`alarm.msgalarmnoticercpt`	Postmaster@localhost
`alarm.msgalarmnoticesender`	Postmaster@localhost

Table A.26 Disk space alarm attributes

Disk Space Attributes	Default Value
`alarm.diskavail.msgalarmstatinterval`	3600 seconds
`alarm.diskavail.msgalarmthreshold`	10%
`alarm.diskavail.msgalarmwarninginterval`	24 hours

Table A.27 Server response alarm attributes

Server Response Attributes	Default Value
`alarm.serverresponse.msgalarmstatinterval`	600 seconds
`alarm.serverresponse.msgalarmthreshold`	10 seconds
`alarm.serverresponse.msgalarmwarninginterval`	24 hours

Alarm Attribute Examples

To modify the `msgalarmnoticercpt` attribute to send warning email to `joe@airius.com`:

```
configutil -o alarm.msgalarmnoticercpt -v joe@airius.com
```

To modify the `msgalarmstatinterval` attribute to monitor disk space every 600 seconds:

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

To modify the `msgalarmthreshold` attribute to send a warning when the server response time is greater than 15 seconds:

```
configutil -o alarm.serverresponse.msgalarmthreshold -v 15
```

Appendix

B

Program Delivery

This appendix explains how to set up Netscape Messaging Server 4.0 to deliver incoming messages to external programs. Because program delivery has significant system security implications, administrators should carefully review and thoroughly understand the security implications before enabling program delivery.

This appendix discusses the following topics:

- About Program Delivery
- Security Considerations
- Enabling the Program Delivery Module
- Using Program Delivery to Handle Incoming Mail
- Program Delivery in Unix Environments
- Program Delivery in NT Environments

About Program Delivery

This section gives general overview information about Netscape Messaging Server 4.0's program delivery feature.

In this section, the term *program* refers to:

- **Unix**. Any executable file (including scripts).

- **NT**. Any Windows application. For example, any file with the filename extension of `.exe`, `.com`, or `.cmd`.

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives, for example putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response.

To accommodate the needs of advanced users who want more sophisticated control over the handling of their mail, Netscape Messaging Server 4.0 offers the ability to deliver mail to external programs that can carry out these additional tasks. This is called *program delivery*. For example:

- **Program delivery can be used to help sort mail.** If you receive a great deal of mail, you might consider using a mail filter that sorts and delivers incoming mail to one or more folders. An automatic filter can usually sort messages based on the sender or topic of the message. With this type of program delivery, messages are delivered to the filtering program as they arrive.

- **Program delivery can also be used as a mail file server.** Some sites have a lot of information that they wish to make publicly available. The most common way to share files on the Internet is to make them available through the File Transfer Protocol (FTP) or the World Wide Web (WWW). But not everyone has FTP or web access. You can make files available to those who only have mail with a file server that selects and mails documents in response to mail requests.

  A request sent to a typical mail file server consists of one or more commands such as this:

  ```
  SEND /documents/internet/rfc/rtc822.txt
  ```

When you or a user specifies program delivery as an account option, as described in Using Program Delivery to Handle Incoming Mail, one or more programs are run whenever mail addressed to that account is received. The Messaging Server starts the program and the mail is handed over to it. The program then performs whatever it is designed to do with incoming messages.

As described in the following sections, an administrator must first enable program delivery on the messaging server. Once program delivery is enabled, users can select one or more programs to be run when messages addressed to their account are received.

Program Delivery and Mailbox Delivery

Program delivery is independent of, and separate from, delivery of messages to the account's mailbox. An account can use one or both. For example, if both POP/IMAP delivery and program delivery are selected, then incoming messages are delivered to the mailbox and also processed by program delivery.

Program Delivery Failures

If an incoming message is addressed to an account using program delivery, and for some reason program delivery fails, the incoming message is returned to the sender and a "delivery failed" type error message is generated. This might occur, for example, if a particular program is designated to handle incoming messages but the program delivery module cannot find that program because it has been moved or deleted from the directory where program delivery expects to find it.

Because program delivery and mailbox delivery are two separate and distinct operations, messages will be bounced back to senders if one fails even though the other succeeds. For example, if an account is using both program delivery and mailbox delivery, and program delivery fails, an incoming message will be bounced back to the sender with an "undeliverable" notice even though a copy of the message may be successfully delivered to the account's mailbox.

Security Considerations

Because users can specify that program delivery automatically execute one or more programs in response to incoming messages, program delivery could compromise system security if not properly administered. For this reason, program delivery is disabled by default and must be explicitly turned on by an administrator as explained in Enabling the Program Delivery Module.

Trusted Programs and Directory

A *trusted* program is one that is assumed to function properly when used with program delivery. Before designating a program as *trusted*, you should carefully inspect it to make sure that program delivery can automatically run it without risking system problems or reducing network security.

The program delivery module looks for trusted programs in a special directory known as the *trusted directory*. Any program or executable file stored in the trusted directory is assumed to be a trusted program. In other words, you designate a program as trusted by storing it in the trusted directory.

The location of the trusted directory cannot be changed. The location of the trusted directory is:

- **Unix**: *server-root*/msg-*instance*/smtp-bin/delivery
- **NT**: *server-root*\msg-*instance*\smtp-bin\delivery

As an administrator, you must ensure that each trusted program is well understood and known to be safe before placing it in the trusted directory. Make sure that every program stored in the trusted directory does nothing that will compromise security. When examining programs for security problems, keep in mind that system security involves more than just keeping messages and data out of unauthorized hands. An innocent mistake in a poorly written or configured program can cause serious system problems.

When running in secure mode, the program delivery module ignores any path specified in the user's account and only runs programs stored in the trusted directory. This allows an administrator to determine the exact executable files the program delivery feature will run.

For example, if Windows NT users want to set up a program delivery application that notifies them when new mail arrives, they can specify it for their account as:

```
\bin\new_mail.exe
```

or simply as

```
new_mail.exe
```

Regardless of how users specify `new_mail.exe`, the program delivery module will only execute the trusted version of `new_mail.exe` that is stored in the trusted program directory. If there is no version of `new_mail.exe` in the trusted directory, program delivery exits with an error message to the mail administrator.

Trusted Directory and Operating Modes

- **NT**. In NT environments, program delivery will only run in secure mode. This means that it will only run programs stored in the trusted directory.
- **Unix**. In Unix environments, program delivery can run in one of two operating modes: *secure* and *non-secure*. In secure mode, program delivery will only run programs stored in the trusted directory. In non-secure mode, program delivery can run programs stored anywhere on the network. See Secure and Non-secure Modes (Unix) for details.

Guarding the Trusted Directory

By default, only administrators with `root` access (Unix), or administrator privileges (NT), can add or change programs in the trusted directory. Netscape recommends that this protection be maintained, and that the permissions for this directory never be relaxed to allow anyone else to add or modify programs in the trusted directory.

In regards to program delivery, the most important aspect of security is preventing unauthorized access to the trusted directory. Because program delivery assumes that any program stored in the trusted directory is secure and safe, it is essential that unauthorized persons are prevented from adding or modifying files in the trusted directory.

Scripts and Batch Files

Unix Environments

In Unix environments, scripts and batch files can be used by program delivery, but extra care should be taken to ensure that they are safe.

Scripts and batch files can run programs that are not stored in the trusted directory. If you use a script or batch file for program delivery, and it calls commands or programs that have not been inspected for safety and stored in the trusted directory, you run the risk of someone substituting or changing that command or program to detrimental effect.

Programs that interpret their input as a sequence of commands to execute (such as `sh`, `tcsh`, or `perl`) should not be used as trusted programs. However, some scripts that run under such programs can be considered safe after careful inspection. For example, it is risky to set up `perl` as a trusted program, but a carefully inspected `perl` script might be safe to use.

NT Environments

In Windows NT environments, Netscape recommends that you do not use scripts or batch files for program delivery.

Enabling the Program Delivery Module

For security reasons, program delivery is disabled by default and must be explicitly turned on by an administrator.

- **Disabled**. If the trusted directory is empty, the program delivery module is disabled and no one can use programs to process incoming mail.
- **Enabled**. If one or more files are stored in the trusted directory, the program module is enabled. If properly set up as described in Setting Up Program Delivery (Unix) and Setting Up Program Delivery (NT), programs can be designated to process incoming mail.

In both Unix and Windows NT environments, you enable the program delivery module by placing one or more programs in the trusted directory.

In Unix environments, there are two additional ways of enabling the program delivery module other than placing an executable file in the trusted directory:

- Store a link to an executable file in the trusted directory.

- Store a non-executable file named `INSECURE-PROGRAM-DELIVERIES` in the trusted directory. Note, however, that the presence of this file causes program delivery to run in non-secure mode which significantly increases security risks. See Secure and Non-secure Modes (Unix) for details.

Using Program Delivery to Handle Incoming Mail

This section describes how to designate one or more software programs to process incoming messages for an account.

To designate programs to handle incoming mail, the program delivery module must first be set up and enabled as described in Setting Up Program Delivery (Unix) and Setting Up Program Delivery (NT).

Once program delivery is set up and enabled:

- An administrator can designate one or more programs to handle incoming mail for any account.
- An account owner can designate programs to process incoming mail for the account.

Administrators

Administrators can specify program delivery for any account. This can be done through the Create User window at the time the mail account is created, or through the Edit User window for an account that already exists.

1. Before establishing program delivery for a user:

   Make sure program delivery has been enabled as explained in Enabling the Program Delivery Module.

   Make sure the programs to be used for this account have been inspected for safety and placed in the trusted directory. (In Unix environments, you can choose to run program delivery in non-secure mode. In that case, the programs do not have to be stored in the trusted directory.)

2. Go to the Create User or Edit User window.

3. Choose Mail from the menu and click on the Delivery tab.

4. Check the box labeled "Program delivery." The Properties button is activated.

   POP/IMAP delivery. If the "Enable POP/IMAP delivery" box is *also* checked, mail will continue to be delivered to the mailbox regardless of program delivery. In other words, if both the "Program delivery" and the "POP/IMAP delivery" boxes are checked, incoming mail will be processed by program delivery and *also* delivered to the mailbox.

   Unix delivery. The "Unix delivery" box has nothing to do with program delivery. Do not check this box simply because you are operating in a Unix environment. For information on when and why to check the "Unix delivery" box, see Configuring Delivery Options in Chapter 4, Managing Mail Users and Mailing Lists.

5. Click the Properties button next to the Program Delivery option. The Program Delivery dialog box is displayed.

6. In the Program Delivery dialog box, enter the command (program) that is to process incoming messages for this account.

   Unix secure mode. When running program delivery in secure mode, you need only enter the command name, you do not need to enter a path. For example, to run the program named `mymail` stored in the trusted directory, you enter `mymail`.

   Unix non-secure mode. When running program delivery in non-secure mode, you must enter an absolute path for the program to run. (Program delivery does not make any use of paths in the account owner's environment.) For example, to run the program named `mymail` stored in the `/usr/bin` directory, you enter `/usr/bin/mymail`.

   NT. You must enter the filename exactly as the filename exists in the trusted directory (including the filename extension). You do not need to enter a path. For example, to run the `mymail.exe` stored in the trusted directory you enter `mymail.exe`. program delivery.

7. To run multiple programs, enter each program on a separate line by itself. Programs will be run in the order you specify. For example, to first run the `new_mail.exe` program, and then the `sort_mail.cmd` program, simply enter:

```
new_mail.exe
sort_mail.cmd
```

8. Now click on OK.

Note: The Messaging Server will allow you to enter the name of a program that has not been placed in the trusted directory (or a program with an incorrect path if running in Unix non-secure mode). But program delivery will fail when it tries to use that program. At that point a "delivery failed" type error message will be sent to the mail administrator and the incoming message bounced back to the sender with an "undeliverable" type notice.

To stop using program delivery to handle incoming messages for this account, simply delete the programs from the dialog box and uncheck the Program Delivery box.

To change the programs that program delivery runs for this account, simply add, delete, or change the programs listed in the dialog box.

Users and Account Owners

End users can designate program delivery for their accounts through the end user Server Account Management forms. To designate one or more programs to handle incoming mail for their accounts, end users should follow these steps:

1. Check with the appropriate administrator to:

   - Make sure program delivery has been enabled for the Messaging Server.
   - Find out if the program (or programs) they want to use have been placed in the trusted directory. (In Unix environments, this may not be necessary if you have set up program delivery to use any program, not just those stored in the trusted directory.)
   - Obtain the machine name and port number of the Administration Server.

2. Go to the Delivery Options window of the Server Account Manager.

3. In the Extra Processing pane of the Delivery Options window, check the box labeled "Filter all incoming messages through one or more programs."

   Note that program delivery is separate from, and independent of, mailbox delivery. If either the "Your POP3/IMAP mailbox" or "Your UNIX mailbox" boxes are *also* checked, mail will continue to be delivered to the end users mailbox regardless of program delivery. In other words, if both the "Filter all..." and the "POP3/IMAP mailbox" boxes are checked, incoming mail will be processed by program delivery and *also* be delivered to the user's mailbox.

4. In the dialog box, enter the command (program) that will process incoming messages for this account:

   Unix secure mode. By default, program delivery runs in secure mode in Unix environments. Check with the administrator to confirm that it is running in secure-mode. Under secure-mode, users need only enter the command name; they do not need to enter a path. For example, to run the program named `mymail` stored in the trusted directory, enter `mymail`.

   Unix non-secure mode. If program delivery is running in non-secure mode, users must enter an absolute path locating the program to be run. (Program delivery does not make any use of the user path as stored in the user environment.) For example, to run the program named `mymail` stored in the `/usr/bin` directory, enter `/usr/bin/mymail`.

   NT. In NT environments, the user must enter the filename exactly as the filename exists in the trusted directory (including the filename extension). Users do not need to enter a path. For example, to run the `mymail.exe` stored in the trusted directory, enter `mymail.exe`.

   To run multiple programs, enter each program on a separate line by itself. Programs will be run in the order you specify. For example, to first run the `new_mail.exe` program, and then the `sort_mail.cmd` program, simply enter:

   ```
   new_mail.exe
   sort_mail.cmd
   ```

5. Click Change.

Note: The Messaging Server will allow users to enter the name of a program that has not been placed in the trusted directory (or a program with an incorrect path if running in Unix non-secure mode). But program delivery will fail when it tries to use that program. At that point an error message is sent to the mail administrator and the incoming message bounced back to the sender with an "undeliverable" type notice.

To stop using program delivery to handle incoming messages for this account, simply uncheck the "Filter all..." box and delete the names of the program, or programs, listed in the dialog box. Then click Change.

To change the programs that program delivery runs for your mail, simply add, delete, or change the programs listed in the dialog box. Then click on Change.

Program Delivery in Unix Environments

This section discusses the following topics:

- Program Delivery and Unix
- How Program Delivery Works (Unix)
- Secure and Non-secure Modes (Unix)
- Setting Up Program Delivery (Unix)
- Suspending Program Delivery (Unix)
- Disabling Program Delivery (Unix)

Program Delivery and Unix

The following factors should be considered when using program delivery in Unix environments:

- **Restricted environment:** Many programs (especially shells such as `/bin/sh` and others) use information from environment variables to modify their behavior. For security reasons, the only environment variables passed to an external program are `TZ` (time zone information), `AGENT=` the Messaging Server (for compatibility with sendmail), and sometimes `PATH`.

- **Setuid-root program:** Some programs need more permissions than those of the user who executes them. Such programs acquire root permissions when they are run. Setuid programs can be identified by an *s* as the user-execute permission in the output of `ls -l`, as shown here:

  ```
  -r-s--x--- 1 root mta 70064 Feb 17 10:32 sort_my_mail
  ```

- **Valid shell:** Before running a program, the login shell of the user the message is addressed to is checked against the list of valid shells found in the `/etc/shells` file. The `/etc/shells` file is simply a list of shells, one per line, that can be used to log into the system. If this file is missing or empty, the user's shell is checked against the following default list:

  ```
  /bin/sh
  /usr/bin/sh
  /bin/csh
  /usr/bin/csh
  /bin/ksh
  /usr/bin/ksh
  ```

  The Messaging Server therefore won't run commands for users who aren't normally allowed to log in and type the commands themselves.

How Program Delivery Works (Unix)

When a program is run in response to an incoming message, that program is run under the user ID of the owner of the account the message is addressed to. For example, if a message is addressed to the `salesdata` account, the program is run under the user ID of the owner of the `salesdata` account. Note, however, that for security reasons, program delivery will not run programs under the `root` user ID. See Specifying the User ID for Root (Unix) for additional information on running programs for the `root` account.

The following algorithm is used to handle incoming mail when program delivery has been specified as a delivery option for incoming mail:

1. The Messaging Server sets up a restricted environment consisting of only the variables `TZ` and `AGENT`.

2. The Messaging Server permanently gives up root permissions by changing to those of the controlling user (using `setuid(2)`). The controlling user is the owner of the account the incoming message is addressed to. If the account is owned by `root`, the controlling user is the designated user as described in Specifying the User ID for Root (Unix)

3. The Messaging Server changes to the controlling user's home directory if possible (it remains in `/tmp` if a failure occurs).

4. The Messaging Server performs two checks:

   - It checks that the program to be run is located in the trusted directory. If the program is not in the trusted directory, it checks the trusted directory for the presence of a file named `INSECURE-PROGRAM-DELIVERIES`. If that file is present, it runs the program as specified by the user with an absolute path. If neither the program nor the `INSECURE-PROGRAM-DELIVERIES` file is present in the trusted directory, program delivery aborts and an error message is sent to the administrator.

   - It makes sure there are no special characters in the command. The special characters it checks for are `$ ^ & ( ) | ` ; < > CR` and `LF`. So, for example, you won't be able to run two programs connected by a pipe. If one of these disallowed characters are present, program delivery fails and the incoming message is bounced back to the sender with an "undeliverable" type notice.

5. The Messaging Server starts the program.

6. The Messaging Server feeds the message to the program.

7. If the user has designated multiple programs, each program is run in the sequence the user specified.

If the program exits abnormally or produces any output, an error message is generated.

Secure and Non-secure Modes (Unix)

See Security Considerations for general security-related information that applies to both the Unix and NT versions of program delivery.

The program delivery module in Netscape Messaging Server 4.0 can operate in one of two security modes:

- **Secure mode**. In secure mode, program delivery will only run the executable files (programs) that are stored in the trusted directory. See Secure Mode for details.
- **Non-secure mode**. In non-secure mode, program delivery will run any executable file (program) stored anywhere on the network. See Non-secure Mode for details.

In this context, an *executable* file is any Unix file with execute permission or a link (hard or soft) to an executable file. In other words, program delivery treats links to programs as if they were the programs themselves.

Netscape recommends that you run program delivery in secure mode. Secure mode allows you as an administrator to specify that program delivery only run those executables that you have examined for security problems and placed in the trusted directory.

Netscape recommends against running program delivery in non-secure mode because in this mode any program anywhere on the network can be used by program delivery and there is no way to ensure that those programs are safe.

Secure Mode

Program delivery runs in secure mode by default.

When running in secure mode, the program delivery module ignores any path specified in the user's account and runs the version of the program that is stored in the trusted directory. This allows the administrator to specify the exact executable files that the program delivery feature will run. If the program is not stored in the trusted directory, program delivery exits with an error message.

For example, if users want to set up a program named `sort_mail` to sort new mail into folders as it arrives, they can specify it in their account as:

```
/usr/local/bin/sort_mail
```

or as

```
sort_mail
```

Regardless of whether or not the user specifies a path, if program delivery is running in secure mode (as Netscape recommends) program delivery will only execute the version of sort_mail in the trusted directory.

Non-secure Mode

When running in non-secure mode, program delivery will run programs stored anywhere on the network, not just those stored in the trusted directory.

Non-secure mode allows any user to have program delivery run any program, or any version of any program. If users can create (or modify) programs for program delivery to automatically run in response to an incoming message, there is no way to ensure that those programs are safe. **Therefore, Netscape cautions that running in non-secure mode endangers system and network security.**

To run program delivery in non-secure mode, simply place a file named `INSECURE-PROGRAM-DELIVERIES` in the trusted directory. The contents of this file do not matter and it does not have to be executable. The name of the file is case-sensitive and must be exactly as shown.

To create this file:

```
touch INSECURE-PROGRAM-DELIVERIES
```

If a file named `INSECURE-PROGRAM-DELIVERIES` is present in the trusted directory, program delivery runs the program identified by the absolute path specified by the user (or administrator). In other words, when program delivery is running in non-secure mode, programs must be qualified by an absolute path in the program delivery dialog box as explained in Using Program Delivery to Handle Incoming Mail.

In non-secure mode, program delivery relies entirely on the specified path. Even if there is a version of the program in the trusted directory, unless the absolute path points to that directory, program delivery will not run it. If no path is specified, or the path is incorrect, program delivery fails and an error message is generated. When program delivery fails, the incoming message is returned to the sender with an “undeliverable” type notice.

To stop running program delivery in non-secure mode and return to secure mode, simply remove the `INSECURE-PROGRAM-DELIVERIES` file from the trusted directory.

Running Programs as root

For security reasons, program delivery will not run programs as `root`. In order to use program delivery for an account owned by `root`, you must designate an alternate user ID to run programs for mail addressed to an account owned by `root`. See Specifying the User ID for Root (Unix) for details.

Setting Up Program Delivery (Unix)

For security reasons, the program delivery module is disabled by default and must be explicitly activated by an administrator who is logged in on the messaging server as `root`.

The administrator must perform the following procedures to set up program delivery:

1. Enable the program delivery module as described in Enabling the Program Delivery Module.

2. Select the programs that program delivery is going to work with, and make sure that they are safe to run.

3. Install the inspected programs in the trusted directory as described in Installing Trusted Programs (Unix) below. (Or if you want to run program delivery in non-secure mode, place a file named `INSECURE-PROGRAM-DELIVERIES` in the trusted directory.)

4. Specify the shells that can be used with program delivery as described in Setting up the List of Valid Shells (Unix) below.

5. If program delivery is going to be used for accounts owned by `root`, designate an alternate user ID under which to run programs as described in Specifying the User ID for Root (Unix).

Once these steps have been completed and program delivery is set up, program delivery can be used to handle incoming mail as described in Using Program Delivery to Handle Incoming Mail.

Installing Trusted Programs (Unix)

Before installing a program in the trusted directory, first inspect it to make sure it is safe for program delivery to automatically run in response to an incoming message.

Then move or copy the inspected program into the trusted directory.

You can use a link in the trusted directory to a program stored somewhere else, but using a link may weaken security. By default, only administrators with `root` privileges can modify or replace a program in the trusted directory, but if you link to a program stored in a directory that grants broader access privileges, you run the risk of someone substituting a poorly written, corrupt, or unauthorized version of the program.

Setting up the List of Valid Shells (Unix)

If you want to allow users with login shells other than `sh`, `csh`, or `ksh` to use the program delivery feature, you need to set up `/etc/shells`.

If you're creating the `/etc/shells` file for the first time, you need to include entries for any of the six default shells that you want to allow.

Here is an example of a `/etc/shells` file:

```
/bin/csh
/bin/sh
/bin/ksh
/usr/bin/sh
/bin/tcsh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/tcsh
```

Specifying the User ID for Root (Unix)

Program delivery will not run programs as `root`. If you are setting up program delivery for a mail account owned by `root`, you must specify an alternate user ID under which to run programs.

To specify the user ID for accounts owned by `root`, follow these steps:

1. Create a special user ID for running programs for mail accounts owned by `root`. For example, a user named `progdel`. Limit the permissions on this account to just those needed to run the programs.

2. Go to the SMTP System Window and enter the user ID for accounts owned by `root` in the Program Deliver pane. For example, enter `progdel` in the Safe user ID for running programs box. See Chapter 3, Configuring SMTP Services. for details.

3. (Optional.) If you wish, you can also specify a group ID for running programs for accounts owned by `root`.

(Note that the pane labeled Unix delivery, has nothing to do with the program delivery module being described in this appendix.)

Suspending Program Delivery (Unix)

You can temporarily suspend all program deliveries by placing a file named `SUSPEND-PROGRAM-DELIVERIES` in the trusted directory. The contents of this file do not matter and it does not have to be executable. The name of the file is case-sensitive and must be exactly as shown.

When program delivery is suspended, incoming messages are not bounced back to the sender, instead they simply queue up waiting for program delivery to be resumed. **Therefore, administrators are cautioned not to suspend program delivery for long periods of time.**

To resume program delivery, simply remove the `SUSPEND-PROGRAM-DELIVERIES` file from the trusted directory.

Disabling Program Delivery (Unix)

To disable program delivery, simple remove all files from the trusted directory.

If program delivery is disabled, messages addressed to accounts that have specified program delivery as a delivery option are bounced back to the sender. This occurs even if the account has also enabled POP/IMAP mailbox

delivery. In other words, if both program mailbox delivery are set up for an account, and all files are removed from the trusted directory, one copy of an incoming message will be placed in the account's mailbox and the message will also be bounced back to the sender with an "undeliverable" type notice.

Program Delivery in NT Environments

This section discusses the following topics:

- How Program Delivery Works (NT)
- Setting Up Program Delivery (NT)
- Suspending Program Delivery (NT)
- Disabling Program Delivery (NT)

How Program Delivery Works (NT)

When a program is run in response to an incoming message, that program is run under the server account specified at installation time. You can also use the SMTP System Window to specify an account to run programs.

The following algorithm is used to handle incoming mail when the program delivery has be specified as a delivery option for incoming mail:

1. Before running a program, the program delivery module performs two checks:

    - It makes sure that the program to be run is stored in the trusted directory. If there is no version of the program in the trusted directory, program delivery exits with an error message to the mail administrator and the incoming message is returned to the sender with an "undeliverable" type notice.

    - It makes sure there are no special characters in the specified command. The special characters is looks for are `$ ^ & ( ) | \ ; < > CR` and `LF`. So, for example, program delivery will not accept two programs connected by a pipe. If one of these disallowed characters are present, program delivery fails and the incoming message is bounced back to the sender with an "undeliverable" type notice.

2. The messaging server runs the trusted program.
3. The messaging server feeds the message to the running program.
4. If the user has designated multiple programs, each program is run in the sequence the user specified.

If the program exits abnormally or produces any output, an error message is generated and the incoming message is bounced back to the sender with an "undeliverable" type notice.

Setting Up Program Delivery (NT)

For security reasons, the program delivery module is disabled by default and must be explicitly activated by an administrator who is logged in to the messaging server with administrator privileges.

The administrator must perform the following procedures to set up program delivery:

1. Enable the program delivery module as described in Enabling the Program Delivery Module.
2. Select the programs that the program delivery module is going to work with and make sure that they are safe to run.
3. Install the inspected programs in the trusted directory as described in Installing Trusted Programs (NT) below.

Once these steps have been completed and program delivery is set up, users can pick the trusted programs that they want program delivery to run when they receive messages. See Using Program Delivery to Handle Incoming Mail for information on how users select program delivery.

Installing Trusted Programs (NT)

You must install in the trusted directory the trusted programs that you want to make available to the program delivery module. First inspect each program to make sure it is safe for program delivery to automatically run in response to an incoming message. Then move or copy the inspected program into the trusted directory.

For example, to enable the program delivery module to use a filter program named `mail-filter.exe`, follow these steps:

1. Make sure that `mail-filter.exe` is safe to run
2. cd *`server-root`*`\msg-`*`instance`*`\smtp-bin\delivery`
3. `copy \bin\mail-filter.exe mail-filter.exe`

Suspending Program Delivery (NT)

You can temporarily suspend all program deliveries by placing a file named `SUSPEND-PROGRAM-DELIVERIES` in the trusted directory. The contents of this file do not matter and it does not have to be executable. The name of the file is case-sensitive and must be exactly as shown.

When program delivery is suspended, incoming messages are not bounced back to the sender, instead they simply queue up waiting for program delivery to be resumed. **Therefore, administrators are cautioned not to suspend program delivery for long periods of time.**

To resume program delivery, simply remove the `SUSPEND-PROGRAM-DELIVERIES` file from the trusted directory.

Disabling Program Delivery (NT)

To disable program delivery, simply remove all files from the trusted directory.

If program delivery is disabled, messages addressed to accounts that have specified program delivery as a delivery option are bounced back to the sender. This occurs even if the account has also enabled POP/IMAP mailbox delivery. In other words, if both program mailbox delivery are setup for an account, and all files are removed from the trusted directory, one copy of an incoming message will be placed in the account's mailbox and the message will also be bounced back to the sender with an "undeliverable" type notice.

Appendix

C

sendmail Migration and Compatibility

Netscape Messaging Server 4.0 includes a `sendmail` emulator program to maintain compatibility with mail programs that employ Unix `sendmail` to deliver their mail. This appendix explains how to move user mail accounts and mail messages from a Unix `sendmail` system to Messaging Server. It also describes the similarities and differences between the Unix `sendmail` application and the Messaging Server `sendmail` emulator.

This appendix includes the following sections:

- Moving Users to Messaging Server
- Moving sendmail Messages to Messaging Server
- Compatibility with Unix sendmail

Moving Users to Messaging Server

To migrate from a Unix `sendmail` system to Netscape Messaging Server 4.0, you need to perform the following procedures:

1. Use the `unix2ldif` utility to convert Unix user account information into an LDIF format file, for example, a file named `file.ldif`. See Running the unix2ldif Utility for a detailed description of this step.

2. If the LDAP Directory already contains data, run the `ldifsplit` utility to split the LDIF file into two different LDIF format files:

   - A file that contains new entries for users that are *not* already in the LDAP Directory.
   - A file that contains the entries for those users who *are* already in the LDAP Directory.

   See Running the ldifsplit Utility for a detailed description of this step.

3. Use the `chkuniq` utility to check for duplicate DNs, user IDs, and email addresses. See Running the chkuniq Utility for a detailed description of this step.

4. Update the LDAP Directory with the user information that is now in the LDIF format files. See Updating the LDAP Directory for a detailed description of this step.

5. Use the `chkuniq` utility to perform a final check for duplicate DNs, user IDs, and email addresses on the LDAP Directory.

6. Use the `MigrateUnixSpool` utility to move messages from users' `sendmail` spool files to the Messaging Server mailbox directories. See Moving sendmail Messages to Messaging Server.

Running the unix2ldif Utility

The `unix2ldif` utility writes your `sendmail` user account information to an LDIF (LDAP Data Interchange Format) file. The `unix2ldif` utility creates one LDAP entry in the LDIF file for each user account. If an account is skipped, the utility gives you a warning. The LDIF file contains the following information:

- user accounts
- mail groups
- forwarding aliases

By default, the `unix2ldif` utility gets its input from the following `/etc` directory files:

- `/etc/passwd`

- `/etc/shadow` (`/etc/security/shadow` on IBM AIX systems.)
- `/etc/aliases` /etc/passwd file.

By default, the `unix2ldif` utility operates on the three `/etc` files listed above. If those are the files that `unix2ldif` is to use, you do not need to explicitly specify the input files with the `-a`, `-p`, or `-s` options. If the input files are not in the `/etc` directory, or if they do not exist at all, or if they have different names, you can use the `-a`, `-p`, or `-s` options to specify the files you want `unix2ldif` to work on. For example, if you want to migrate your users in stages, you could create input files containing just a subset of users and then run `unix2ldif` on those files using the `-p`, `-s`, and `-a` options.

Note that `unix2ldif` can also read SunOS and Solaris NIS map files once they've been converted to ASCII format as described in unix2ldif and NIS Maps.

The `unix2ldif` utility is located in *`server-root`*`/bin/msg/admin/bin`

To run the utility, run the following command:

```
unix2ldif -b dn -d domain [options] > file.ldif
```

The `-b` *`dn`* and `-d` *`domain`* parameters are required. You can name the `unix2ldif` output file whatever you want (this document uses the name `file.ldif`).

The command-line options for `unix2ldif` are described in Table C.1.

Table C.1 unix2ldif options

Option	Description
`-a` *`file`*	For specifying an absolute path and name for the `aliases` input file. To specify no file, use `/dev/null`. Use this option if the aliases file: • does not exist • is not `/etc/aliases`
`-b` *`dn`*	**Required.** The base DN (distinguished name) to use in each DN constructed. To specify no DN, use empty double quotes (" "). For more information about the base DN, see your Directory Server documentation.

Table C.1 unix2ldif options

Option	Description
`-d` *`domain`*	**Required**. The address completion domain. This specifies the domain name that will be to the right of the `@` in each user's email address. For example, to specify that each user's email address is in the form: *`user`*`@airius.com`, you would use the option `-d airius.com`. You can use the `-d` option multiple times in a single command to produce multiple addresses for each user. The first address appears as the mail attribute; the other addresses appear as `mailAlternateAddress` attributes. See Address and Host Completion Domains for additional information.
`-D` *`domain`*	The host completion domain; `host` becomes `host.domain`. The default is the first value given for the `-d` option. Used to complete host names found in the `aliases` file. See Address and Host Completion Domains for additional information.
`-f`	Create forwarding-only entries in LDAP. Use for unresolved, single-target aliases from the `aliases` file.
`-F`	Create forwarding-only entries in LDAP. Use for all unresolved aliases in the `aliases` file.
`-g`	Create group entries in LDAP. Use for unresolved, multi-target aliases in the `aliases` file.
`-G`	Create group entries in LDAP. Use for all unresolved aliases in the `aliases` file.
`-h` *`host`*	The `mailHost` value to use for each user when no value can be derived from the `aliases` file. By default, `unix2ldif` relies on the `aliases` file for this information. See Routing Aliases for additional information regarding this option.
`-H` *`host`*	An alternative to `-h`, `-H` forces the `mailHost` values for all users to be the value specified by *`host`*. This value cannot be overridden by the `aliases` file. See Routing Aliases for additional information regarding this option.
`-m`	Turn off the automatic inclusion of `maildeliveryoption: mailbox` in the `ldif` entry.
`-n`	Turn off the automatic migration of `.forward` information for all users.

Table C.1 unix2ldif options

Option	Description

`-o`	Represent each forwarding-only entry in the directory as an organizational person. With this option, the object classes of the forwarding-only entries will be:
	
	`objectclass: top`
	`objectclass: person`
	`objectclass: organizationalPerson`
	`objectclass: inetOrgPerson`
	`objectclass: mailRecipient`
	`objectclass: nsMessagingServerUser`
	
	Without this option, forwarding-only entries will have only these object classes:
	
	`objectclass: top`
	`objectclass: mailRecipient`
	`objectclass: nsMessagingServerUser`
	
	If you represent the forwarding-only entry as an organizational person, the entry will show up in the Administration Server's User/Group UI under Users. Otherwise, the entry does not show up in the Administration Server's User/Group UI at all.

`-p` *`file`*	For specifying an absolute path and name for the `passwd` input file. Use this option if the password file is not `/etc/passwd`.
`-s` *`file`*	For specifying an absolute path and name for the `shadow` input file. Use this option if the shadow file: • does not exist • is not `/etc/shadow` (or `/etc/security/shadow` in AIX environments) To specify no file, use `/dev/null`.
`-v` *`string`*	An attribute of the form `attr: value` to include with each LDAP user entry constructed. To include individual user names (`uid`) in the string, use a percent sign (`%`) in the string where you want the user name to be. You can have up to four `%` signs for each `-v` option; however, you can have as many `-v` options as you need. This option is available for LDAP person entries only; it is not available for forwarding-only or group entries.

Table C.1 unix2ldif options

Option	Description
`-u`	Use the user ID (`uid`) for creating a DN for a user entry. The default is `cn`.
`-z`	Turn on debugging mode.

Routing Aliases

A routing alias for a user can be in the format `user: user@hostname` or the format `user@hostname.HostCompletionDomain`. For example, `esperanza: esperanza@sirius` or `esperanza@sirius.airius.com`. The user ID and the user portion of the routing alias must match exactly (case-sensitive match).

The `unix2ldif` utility determines how to set the `mailHost` value as follows:

- If the `-H` option is used to specify a host name, that host name is used to set the `mailHost` value. When the `-H` option is used, the `aliases` file is not used to determine how to set `mailHost`. (See unix2ldif and aliases Files for additional information on `aliases` files.)
- If the `-h` option is used to specify a host name, that host name is used to set the `mailHost` value for users who do not have a routing alias in the `aliases` file. Users that do have a routing alias in the `aliases` file have that alias used as their `mailHost` value.
- If neither the `-H` nor the `-h` options are used to specify a host name, `unix2ldif` obtains the `mailHost` value from the `aliases` file.

`HostCompletionDomain` is defined by the `-D` option as explained in Using the -D Option to Set the Host Completion Domain.

Address and Host Completion Domains

This section describes how to use the `-d` and `-D` address and host completion domain options.

Using the -d Option to Set the Address Completion Domain

The `-d` option is used to set the address completion domain(s). Address completion domains are used to generate the email addresses of a given user.

You can use `-d` more than once on a single command line to set several address completion domains. If you use more than one `-d` option, the first one is considered to be the primary domain. For example, to specify two address completion domains named `airius.com` and `other.com`, you enter:

```
unix2ldif -b dn -d airius.com -d other.com > file.ldif
```

For the user ID `lincoln`, this results in the following email addresses:

```
mail:lincoln@airius.com
mailAlternateAddress: lincoln@other.com
```

In this example, `lincoln@airius.com` is the primary address.

Address completion domains are also used to generate more addresses for the user if the user has one or more nickname aliases in the `aliases` file. (See unix2ldif and aliases Files for additional information on `aliases` files.)

Nicknames can be in the form *`nickname`*`: `*`user`*, where *`user`* is the user ID. Recursive nickname aliases are also recognized, for example, *`othername`*`: `*`nickname`*. Using the example address completion domains shown above, if `lincoln` has the nicknames `abe: lincoln` and `my_captain: abe` in the `aliases` file, the following email addresses are generated:

```
mail:lincoln@airius.com
mailAlternateAddress: lincoln@other.com
mailAlternateAddress: abe@airius.com
mailAlternateAddress: abe@other.com
mailAlternateAddress: my_captain@airius.com
mailAlternateAddress: my_captain@other.com
```

Using the -D Option to Set the Host Completion Domain

The `-D` option is used to set the host completion domain. If `-D` is not used, `unix2ldif` uses the primary address completion domain (the value specified with the `-d`) as the host completion domain.

The host completion domain is used as follows:

- When determining whether an `aliases` file entry is a routing alias of the form *`user@host.HostCompletionDomain`*, `unix2ldif` uses the host completion domain as defined here in the comparison (see Routing Aliases for more information on routing aliases, and unix2ldif and aliases Files for additional information on `aliases` files.)

- When formulating a user's `mailHost` value, if the information is a host name with no dot because the user's routing alias was *`user@hostname`*, or the `-H` or `-h` options were used with a *`host`* value with no dot, then `unix2ldif` appends a dot and the host completion domain to get the fully-qualified host name for the `mailHost` value. For example, if `-h sirius` is used and the *`HostCompletionDomain`* is `airius.com`, the `mailHost` value becomes `sirius.airius.com`.

- When creating a Forwarding Alias LDAP entry or a Mail Group LDAP entry, the forwarding target or group member is specified as *`user@hostname`* (where *`hostname`* is a host name with no dot). The *`HostCompletionDomain`* is then added to complete the entry in the format: *`user@hostname.HostCompletionDomain`*.

Note that *`HostCompletionDomain`* is not applied to addresses found in a user's `.forward` file when creating a user LDAP entry and reading the `.forward` file to find forwarding addresses. Forwarding addresses read from a user's `.forward` file must be of the form *`something@domain`*, where *`domain`* is a DNS domain string containing at least one dot.

unix2ldif and aliases Files

When `unix2ldif` reads an `aliases` file, each entry is assumed to be in one of two forms:

```
key: value
key value
```

The *`key: value`* form is typical of `/etc/aliases` files, the *`key value`* form is typical of the output of `ypcat -k aliases` which dumps the NIS `aliases` map as explained in unix2ldif and NIS Maps. Any spaces between the colon and the value in the `/etc` form are ignored. No leading spaces are allowed before the *`key`*, but spaces are allowed within the *`key`*. Spaces are not allowed between the *`key`* and the colon (`:`) in the `/etc` form. Trailing white spaces after *`value`* are allowed but ignored.

The `:include` directive is not supported. If this directive is used in an `aliases` file, the results are undefined.

If there is more than one alias with the same key, this is considered to be invalid, and the results are undefined.

The *`value`* may contain one target. For example: `name: miyoko`. Or the *`value`* may contain multiple targets. For example: `name: miyoko`, `hirokani`, `atemi`. A comma is used to separate multiple targets. White space before or after a comma is allowed, but is ignored.

Each target must be a valid email address. For example: `sarah`, `sarah@antares`, `sarah@antares.airius.com`, `sarah@airius.com`.

Alias targets that contain certain unexpected characters such as: `# & / % |` (for example, `/dev/null`) are ignored. In such cases, the alias is still used if any usable targets are present.

The `unix2ldif` utility makes multiple passes through an `aliases` file. If an alias is selected in a given `unix2ldif` pass, it is not used in subsequent passes. The aliases are used as follows.

Pass 1. When creating user accounts for each user ID found in the `passwd` file, `unix2ldif` checks to see if an alias has a key equal to the user ID. If so, it considers it selected in this pass (and not available in subsequent passes). If the `-H` option was not used, and the alias fits the form of a routing alias (as discussed in Routing Aliases), it is used to determine the user's `mailHost` value, but otherwise, the alias is not used.

Pass 2. When creating user accounts for each user ID found in the `passwd` file, `unix2ldif` checks to see if there are any nickname aliases for the user ID. If so, they are used to generate addresses.

Pass 3. Remaining single-target aliases are used to create `Forwarding Alias` entries if the `-f` or `-F` options were specified. Or `Mail Group` entries if the `-G` option was specified. Remaining multi-target aliases are used to create Forwarding Alias entries if the `-F` option was specified, or Mail Group entries if the `-g` or `-G` options were specified.

Unexpected results may occur if there are conflicts between user IDs and aliases. For example, if `chou` and `wong` are both user IDs in the `passwd` file, and there is an alias `chou: wong`, unexpected results may be produced. (It is

considered unexpected that aliases are being used to forward from one `passwd` file user account to another `passwd` file user account because this is ordinarily done with `.forward`).

At the end of its run, `unix2ldif` outputs those aliases that were not used.

unix2ldif and passwd Files

A `passwd` file entry is considered by `unix2ldif` as a valid `passwd` file user account if all of the following are true:

- None of the following fields are empty: user ID, password, gecos (full name), and home directory.
- The encrypted password string is 13 characters. The `unix2ldif` utility first checks the password field in the `passwd` file, and if the field is not 13 characters long, it checks the `shadow` file where the password string must be 13 characters long.
- The user has a mail host. That is, the user has a routing alias in the `aliases` file, or the `-h` or `-H` options were specified.

If the passwd entry is valid, an LDAP user entry is created for the user in the `unix2ldif` output file.

unix2ldif and NIS Maps

The `unix2ldif` utility can also read Network Information Service (NIS) map files.

If your NIS environment **does not include** `/etc/shadow` files (or `/etc/security/shadow` files in AIX environments), follow these steps to run `unix2ldif` on NIS maps:

1. Use `ypcat` to copy the NIS map data to ASCII files as follows:

```
ypcat passwd > /tmp/passwd.txt
ypcat -k aliases > /tmp/aliases.txt
```

2. Run `unix2ldif` on the two `/tmp/*.txt` files you just created.

```
unix2ldif -b dn -d domain -p /tmp/passwd.txt \
-s /dev/null -a /tmp/aliases.txt > file.ldif
```

If your NIS environment **does include** `/etc/shadow` files (or `/etc/security/shadow` files in AIX environments), follow these steps to run `unix2ldif` on NIS maps:

1. Use `ypcat` to copy the NIS map data to ASCII files as follows:

```
ypcat passwd > /tmp/passwd.txt
ypcat shadow > /tmp/shadow.txt
ypcat -k aliases > /tmp/aliases.txt
```

2. Run `unix2ldif` on the three `/tmp/*.txt` files you just created.

```
unix2ldif -b dn -d domain -p /tmp/passwd.txt \
 -s /tmp/shadow.txt -a /tmp/aliases.txt > file.ldif
```

If your NIS environment does not use a `shadow` file, and therefore you do not have a `shadow.txt` file, use `-s /dev/null` instead of `-s /tmp/shadow.txt`.

Running the ldifsplit Utility

The `ldifsplit` utility takes the LDIF file created by the `unix2ldif` utility (*`file`*`.ldif`) and splits it into two files:

- A file of LDAP entries that are already in the directory (the DN already exists). You can name this file whatever you want (this document uses the name `mod.ldif` because it will be used to modify the existing LDAP Directory entries).
- A file of LDAP entries that are not already in the directory (no DN exists). You can name this file whatever you want (this document uses the name `add.ldif` because it will be used to add new entries to the LDAP directory).

If your LDAP Directory is empty, you do not need to run `ldifsplit`. But if your LDAP Directory already contains user account information, running `ldifsplit` at this time may prevent later problems.

The `ldifsplit` utility is located in *`server-root`*`/bin/msg/admin/bin`.

To run the `ldifsplit` utility, follow these steps:

1. Export the contents of your LDAP server instance into an LDIF file. You can name the export file whatever you want (this document uses the name `existing.ldif`). See your Directory Server documentation for details on how to export a directory server instance.

2. Run the `ldifsplit` utility using the following syntax (assuming that the `unix2ldif` output file is named `file.ldif` and the LDAP Directory export file is named `existing.ldif`):

   ```
   ldifsplit -f file.ldif -e existing.ldif -a add.ldif -m mod.ldif
   ```

   With this syntax, `ldifsplit` compares the `unix2ldif` output file (`file.ldif`) to the existing contents of the LDAP Directory as contained in the export file (`existing.ldif`). The utility then creates two new files:

   - `mod.ldif` containing entries for users who are already in the LDAP Directory.
   - `add.ldif` containing new entries that are not in the LDAP Directory

3. Check the `add.ldif` and `mod.ldif` files to see if they contain any entries.

   ```
   tail add.ldif
   tail mod.ldif
   ```

   If a file is empty, you do not need to do anything with it.

   If either the `add.ldif` file or the `mod.ldif` file contains data, that data needs to be written into the LDAP Directory as described in Updating the LDAP Directory.

The command-line options for `ldifsplit` are described in Table C.2.

Table C.2 ldifsplit options

Option	Description
`-a` *`add`*`.ldif`	Name of file containing new entries to be added.
`-e` *`existing`*`.ldif`	Name of the file containing the data that currently exists in the LDAP Directory server instance.

Table C.2 ldifsplit options

Option	Description
`-f` *`file`*`.ldif`	Name of the `unix2ldif` output file.
`-m` *`mod`*`.ldif`	Name of file containing LDAP entries that ned to be modified in the LDAP Directory.

Running the chkuniq Utility

The `chkuniq` utility checks the output files of the `unix2ldif` and `ldifsplit` utilities and the contents of the existing LDAP Directory for duplicate entries. It checks the specified files for

- duplicate DNs
- duplicate user IDs
- duplicate email addresses

The `chkuniq` utility is located in *`server-root`*`/bin/msg/admin/bin.`

The steps that follow describe how to eliminate duplicate entries before writing data to the LDAP Directory.

(Note: The steps below assume that you used `ldifsplit` to create the `add.ldif` file as described in Running the ldifsplit Utility. If you did not run `ldifsplit`, then run `chkuniq` on the `unix2ldif` output file (`file.ldif`) rather than `add.ldif`.)

1. Use `chkuniq` to make sure that the `add.ldif` file (or `file.ldif`) is internally consistent with no duplicates.

   ```
   chkuniq add.ldif
   ```

2. Use `chkuniq` to make sure that the `existing.ldif` file is internally consistent with no duplicates. (The `existing.ldif` file is created by exporting the current contents of the LDAP Directory to a file named `existing.ldif`.)

   ```
   chkuniq existing.ldif
   ```

3. Use `chkuniq` to compare the `add.ldif` file and `existing.ldif` files against each other.

```
chkuniq add.ldif existing.ldif
```

When `chkuniq` finds a duplicate, it reports that to standard output. Or you can use `> filename` to redirect output to a file.

There is no output if chkuniq does not find any duplicates.

If `chkuniq` reports duplicates or errors, inspect your files and correct and resolve all problems before writing data to the LDAP Directory as described in Updating the LDAP Directory. (The most common cause of duplicates are errors in the `passwd` and `aliases` files that were given to `unix2ldif` as input.)

The command-line syntax options for the `chkuniq` utility are described in Table C.3.

Table C.3 chkuniq options

Syntax	Description
`chkuniq file1`	Check for duplicates within *file1*.
`chkuniq file1 file2`	Check for duplicates among *file1* and *file2*.

Updating the LDAP Directory

The final stage of moving users from a Unix `sendmail` system to Netscape Messaging Server is to update the LDAP Directory with the account information converted from `sendmail`.

- If you ran `ldifsplit` to create `add.ldif` and `mod.ldif` files, update the LDAP Directory from each of those two files.
- If you did not run `ldifsplit`, update the LDAP Directory from the `file.ldif` file created by `unix2ldif`.

There are two ways to update the LDAP Directory from the LDIF files:

- **Database Manager**. The Netscape Directory Server provides a Database Manager that can be used to update the LDAP Directory as described in Updating the LDAP Directory with Database Manager.

- **`ldapmodify`**. You can also use the `ldapmodify` command-line utility to update the LDAP Directory as described in Updating the LDAP Directory with ldapmodify.

Updating the LDAP Directory with Database Manager

You can use the Database Manager feature to write the user account information in the LDIF files to the LDAP Directory instance on the Directory Server.

To update the LDAP Directory instance with the Database Manager, follow these steps:

1. Make sure the Directory Server is running.
2. Log in to the Directory Server. You must have read and execute permission to use Database Manager and read and write permissions for the targeted entries in the LDAP directory. (You can run this remotely using `-h` *`host`*.)
3. Go to the Database Manager screen as described in your Directory Server documentation.
4. Select the Add Entries form.
5. In the Full Path to LDIF File field, enter the full path name to the LDIF file that contains the entries you want to add.

   If you created `add.ldif` and `mod.ldif` files by running `ldifsplit`, enter the full path and name of the `add.ldif` file. For example, if you ran `ldifsplit` in the `/tmp` directory: `/tmp/add.ldif`. Then repeat the process for `mod.ldif`.

   If you did not run `ldifsplit`, enter the full path and name of the `unix2ldif` output file. For example: `/tmp/file.ldif`.
6. Leave the Bind to Server field as is.
7. The Password field should already contain the correct password.
8. Choose Okay. The entries are added to your Directory Server manager.

Updating the LDAP Directory with ldapmodify

You can use the `ldapmodify` command-line utility to write the `sendmail` user account information in the LDIF files to the LDAP Directory instance on the Directory Server.

The `ldapmodify` utility is located in *`server-root`*`/userdb/ldap/tools`.

To update the LDAP Directory with `ldapmodify`, follow these steps:

1. Make sure the Directory Server is running.
2. Log in to the Directory Server system as `root`.
3. Go to the directory containing the LDIF files.
4. Run `ldapmodify` to update the LDAP Directory:

   If you created `add.ldif` and `mod.ldif` files by running `ldifsplit`, run `ldapmodify` on both files:

   ```
   ldapmodify -f mod.ldif
   ldapmodify -a -f add.ldif
   ```

   If you did not run `ldifsplit`, run `ldapmodify` on the `unix2ldif` output file. For example: `file.ldif`

   ```
   ldapmodify -a -f file.ldif
   ```

Moving sendmail Messages to Messaging Server

Before users can access their messages with Netscape Messaging Server 4.0, their messages must be moved from the `sendmail` spool file to their Messaging Server mailbox with the `MigrateUnixSpool` utility. This is done with the `MigrateUnixSpool` command-line utility.

Running the MigrateUnixSpool Utility

The `MigrateUnixSpool` utility reads messages from the user's `sendmail` mailbox and appends them to the user's Messaging Server mailbox.

Administrators can use the `MigrateUnixSpool` utility to move users' messages for them. Netscape recommends that administrators move messages for users rather than having users move their own messages. To do this, the administrator must be an authorized mail store administrator. When administrators run `MigrateUnixSpool` to move messages for others, they must use the `-a` and `-v` options.

Although users can run the `MigrateUnixSpool` utility to move their own messages from their `sendmail` spool file to their Messaging Server mailbox, Netscape recommends *against* having users move their own messages. If users run `MigrateUnixSpool` for themselves, they do not use the `-a` and `-v` options.

`MigrateUnixSpool` is located in *`server-root`*`/bin/msg/admin/bin`.

`MigrateUnixSpool` is run with the following syntax:

```
MigrateUnixSpool -u uid -o mailspool -d destmailhost
  -a admin -v password -m destmaildrop
```

The command-line syntax options for the `MigrateUnixSpool` utility are described in Table C.4.

Table C.4 MigrateUnixSpool options

Option	Description
`-a` *`admin`*	The user ID of the administrator running `MigrateUnixSpool` on *`destmailhost`*
`-d` *`destmailhost`*	The destination mail server.
`-h`	Invokes help for this command.
`-m` *`destmaildrop`*	The name of the partition where the user's account is to be created.
`-o` *`mailspool`*	The mail spool path on the source mail server.

Table C.4 MigrateUnixSpool options

Option	Description
`-u` *`uid`*	The user ID of the user whose mailbox needs to be moved.
`-v` *`password`*	The password for the administrator running `MigrateUnixSpool` on *`destmailhost`*

MigrateUnixSpool Example

In this example, an administrator logged in as `admin` moves the spool file for someone with the user ID `lincoln` to the Messaging Server host `mailserver` in the `primary` partition.

```
MigrateUnixSpool -u lincoln -o /var/mail/lincoln -d mailserver
   -a admin -v password -m server-root/msg-instance/store/partition/
   primary
```

Compatibility with Unix sendmail

In order to maintain compatibility with Unix applications and processes that make use of the Unix `sendmail` command, Netscape Messaging Server 4.0 includes its own `sendmail` program that replaces the Unix `/usr/lib/sendmail` software.

Command-line Compatibility

The Messaging Server includes a program named `sendmail` that emulates the Unix `sendmail` program in the `/usr/lib` directory. Most of Unix `sendmail`'s functionality is performed by one or more modules in the Messaging Server, so the `sendmail` emulator is primarily for compatibility with many mail programs that employ Unix `sendmail` (rather than SMTP) to deliver their mail. The Messaging Server `sendmail` emulator program can also be used to start up the Messaging Server mail system and to check and deliver the mail queue.

Sending Mail with the sendmail Emulator

The Messaging Server `sendmail` emulator maintains compatibility with existing software that delivers mail using the Unix `sendmail` command.

Some examples of `sendmail` emulator commands that work for sending mail are:

```
/usr/lib/sendmail -t < /tmp/message
cat file1 | /usr/lib/sendmail -oem recip1,recip2
```

For a complete list of command-line options and options related to sending mail, see Sendmail Emulator Options and Aliases.

Starting the Messaging Server with sendmail

Because Unix `sendmail` comes installed on most Unix-based machines, many scripts, such as system boot scripts, exist to start up `sendmail`. This is done with a command such as:

```
/usr/lib/sendmail -bd -q30m
```

The Messaging Server `sendmail` emulator recognizes this command and starts up the Messaging Server if it isn't already running. The `-q30m` option is ignored.

Checking the Mail Queue with mailq

Some system administrators are used to typing `mailq` to check for queued messages. The `sendmail` emulator provided with the Messaging Server will respond to this command with the contents of the mail queue. However, many server administrators now prefer to use the Messaging Server mail queue form, which makes processing the queue easier.

To check the mail queue with the `sendmail` emulator program, type `mailq` at a command prompt. If there are no queued messages, that fact will be reported.

If there are queued messages, each host that has queued messages waiting to be delivered will be listed, along with the number of pending deliveries.

Other Modes

The Unix `sendmail` program has several other operating modes that aren't necessary or are not supported by the Messaging Server. For a complete list of supported operating modes and command-line options and options, see Functional Compatibility.

Functional Compatibility

The following sections specify the differences between Unix `sendmail` and the Messaging Server `sendmail` emulator with regard to SMTP, aliases and mail forwarding, program delivery, file delivery, and mailing lists.

For information about how Netscape Messaging Server routes messages, see the chapter titled Message Routing.

Network Interface

The Messaging Server is preconfigured for interacting with other machines on the Internet.

In contrast, the Unix `sendmail` program needs to exchange mail with remote destinations using SMTP. Mail routing is achieved with rule sets containing address production rules written in a specialized programming language used to take addresses apart and put them back together in useful ways. Although this is a very powerful facility, it is error prone and requires extensive knowledge of Internet standards to set it up correctly.

Aliases and Mail Forwarding

Unix `sendmail` supports several types of aliases in the `/etc/aliases` file and in users' personal `.forward` files. The various types of aliases allow:

- local users to receive mail at several addresses
- messages to be distributed to multiple recipients
- messages to be forwarded to users at other machines

With Messaging Server, each type of alias is created differently because of the structure of user accounts in the Directory Server database.

Delivery to Programs

Using Unix `sendmail`, you can create an alias or forward that delivers incoming mail to a program. The program then reads the mail and performs some operation depending on the mail contents. These types of programs usually filter messages into different mailboxes or send out automatic replies such as vacation notices. This functionality makes it easy to extend the mail system, but is problematic with respect to security.

You can use the Server Account Management window to set up Messaging Server program delivery for a particular user. However, because there are security issues specific to program delivery, program delivery is disabled by default. See the chapter titled "Program Delivery" for information on how to enable Messaging Server program delivery.

Delivery to Files

Unix `sendmail` makes it possible to set up an alias or `.forward` file to append mail to a file. This can be used to keep a record of incoming mail or to delete incoming mail by sending it to `/dev/null`. However, for delivery-to-file needs the author of `sendmail` recommends using an alternate delivery agent invoked through the delivery-to-program facility.

The Messaging Server's `sendmail` emulator will append undeliverable messages to users' `dead.letter` files, for users with Unix Delivery enabled. No general delivery-to-file facility is planned for the Messaging Server; appending mail to a file should be with the delivery-to-program facility as described in the appendix titled "Program Delivery."

Mailing Lists

Mailing lists in Unix `sendmail` are implemented using aliases and program deliveries. List recipients are stored either in the aliases database or in an external file using an `:include:` alias. Several mailing-list administration programs are available that can automate the task of maintaining recipient distribution lists, while `sendmail` handles the delivery of the messages.

With Messaging Server, you create groups with the Netscape Console.

Sendmail Emulator Options and Aliases

Table C.5 in this section lists the alias names you can use to run the Messaging Server `sendmail` emulator program. Table C.6 lists and describes the available command-line arguments that the `sendmail` emulator program recognizes. Certain options are recognized (through the `-o` command-line option), and their effects are described in Table C.7.

Alternate Names for sendmail

You can run the Unix `sendmail` program under several names as a shorthand way to specify the action to perform. The Messaging Server `sendmail` emulator program recognizes several of these alternate names. The behavior that results from invoking the `sendmail` emulator with an alternate name is summarized in Table C.5.

Table C.5 Invoking sendmail with alternate names

Name	What running under this name does
`bsmtp`	Prints an error message because batch SMTP is not supported.
`mailq`	Reports the contents of the mail queue.
`newaliases`	Prints an error message because the `aliases` file is not used.
`sendmail`	Sends a single mail message.

Note that the result described in Table C.6 will result if no other result is specified using a command-line option such as `-b` or `-I`.

Command-line options are processed using `getopt(3)` as in V8 `sendmail`. All the options supported by V8 `sendmail`, IDA sendmail, and other versions of `sendmail` are recognized; the extent of support for these options is given in Table C.6.

Table C.6 sendmail emulator program command-line options

Option	Description
`-B7`	If set to 7 bit, the high bit is stripped from every byte of the input message.
`-b`*x*	Changes the mode of operation. Where *x* is one of the following: The following modes are supported: `-be` Starts the Messaging Server mail system. `-bm` Sends a single mail message. `-bp` Shows the status of the mail queue. These modes are recognized but not supported: `-ba` Uses Arpanet protocols. `-bb` Does batch SMPT on standard input. `-bi` Initializes the aliases database. `-bs` Does SMTP on standard input. `-bt` Goes into address-testing mode. `-bz` Freezes the configuration.
`-C`	None. There is no configuration file, so this option is ignored.
`-c`	None. This option is obsolete.
`-d`	None. This option is ignored because there is no debug mode.
`-e`	Sets the error-reporting mode (see option `e` in Table C.7).
`-F`	Sets the full name of the sender. If the user running `sendmail` isn't `root`, `daemon`, `UUCP`, `SMTP`, `mail`, or `sendmail`, a header is added to the message indicating the actual sender.
`-f`	Sets the email address of the sender. The same precaution is taken as in the `-F` option.
`-h`	None. The hop count is determined by counting the number of received headers in the message.
`-I`	Runs as if invoked as `newaliases`, which just prints an error message.
`-i`	None. This is the default behavior. If `sendmail` is run interactively, a single "." (`.`) will end the message. If it is run non-interactively (for example, through a pipe to standard input), the end-of-file condition determines the end of the message.

Table C.6 sendmail emulator program command-line options (Continued)

Option	Description
`-M`	The entire queue is processed regardless of the specified Message ID.
`-m`	None. This is the default behavior. The sender is never removed from the list of recipients if it is listed as a recipient.
`-n`	None. This option is not supported.
`-o`	Sets an option. See Table C.7 for a list of supported options.
`-p`	None. This option is not supported.
`-q`	The deferred message queue is processed. If a time interval is given (for example, `sendmail -bd -q30m`), this option is ignored. When this option is specified as `-qR`, `-qS`, or `-qI` (as in V8 `sendmail`), then the behavior is the same as `-R`, `-S`, or `-M`, respectively.
`-R`	Attempts to process the queue for hosts matching the pattern provided (for example, `sendmail -Rabc` will start delivery of queued messages for all hosts containing the string `abc`).
`-r`	Same as `-f` option.
`-S`	The entire queue is processed regardless of the specified sender.
`-s`	None. This option is obsolete.
`-T`	None. This option is obsolete.
`-t`	Recipients are gathered from both the command line and the message header, and the message is delivered.
`-v`	Output is more verbose when sending mail.
`-x`	None. This is an illegal option that is recognized only to prevent printing an error message.
`-Z`	None. There is no frozen configuration file (or even a regular configuration file).

Options for sendmail

The Messaging Server `sendmail` emulator doesn't need a configuration file (`sendmail.cf`), yet most of Unix `sendmail`'s options can be set from the command line. Many of the options are meant for the `sendmail` daemon, but some of them are relevant to the normal operation of sending mail.

All the options supported by V8 `sendmail` are recognized, and the extent of the support for these options is shown in Table C.7. The options listed in Table C.7 refer only to the `sendmail` emulator, not to Messaging Server as a whole. Many of the options not supported by the `sendmail` emulator are supported by the Messaging Server in one way or another. Refer to the relevant sections of this guide to determine how to set parameters within the Messaging Server.

Table C.7 Options supported by V8 sendmail

Option	Description
`7`	If set, the high bit is stripped from every byte of the input message. Also see the `-B` command-line option.
`B`	This is always set to "." (period) and cannot be changed.
`d`	None. Because messages are always posted to the local SMTP server, the turn-around time is fairly quick, so the "i" or interactive mode is always used. However, support for other delivery modes may be added in the future.
`e` *mode*	Changes the error-reporting mode. Valid modes are `e`, `m`, `p`, `q`, and `w`. The behavior for each mode is the same as with Unix `sendmail`. However, if the local SMTP server is unavailable for some reason and mode `m` is chosen, the error message will not be deliverable either. In this case, the message is saved in the sender's `~/dead.letter` file.
`f`	None. When a "From:" line is received, it is changed to "X-Unix-From:" so that it will be RFC822 compliant.
`i`	None. See the `-i` command-line option for details.
`o`	None. This is the default behavior and cannot be disabled.
`v`	Turns on verbose output. Also see the `-v` command-line option.
Others	No other options have any effect. All other options, even invalid ones, are ignored.

Appendix

D

SNMP MIB

The Netscape Management Information Base (MIB) for Messaging Server stores the server information that administrators manage through the Simple Network Management Protocol (SNMP).

This appendix describes the Messaging Server SNMP MIB and provides its complete text. For information about SNMP in Netscape Messaging Server 4.0, see Using SNMP in Chapter 10, Monitoring and Maintaining Your Server.

This appendix contains the following sections:

- About the Messaging Server MIB
- How the MIB Is Activated
- Format of MIB Entries
- Description of the MIB File
- The Messaging Server MIB

About the Messaging Server MIB

The Messaging Server Management Information Base (MIB) is a private SNMP MIB module designed for Netscape Messaging Server 4.0.

Using SNMP with network management software, such as HP OpenView, server administrators can manage Netscape Messaging Server as a network element, performing remote monitoring and data exchange between servers. The SNMP MIB allows the server to monitor server statistics, query static variables, and notify the management station of Messaging Server events.

Each installation of SNMP has its own MIB, a database or information store with a tree-like hierarchy that contains definitions of managed objects, or variables, that store network information for the server. The most general information about the network is at the top level of the hierarchy. Each level below contains information that describes specific parts of the network. For detailed information about MIB structure, see RFC 1155.

Messaging Server's private Messaging Server MIB file, named `netscape-mail.mib`, contains the definitions for variables that store network information for Messaging Server. The MIB is installed during Messaging Server installation in the *`ServerRoot`*`/plugins/snmp` directory. Its shared object identifier is `enterprises 1450`.

You can view the information in the Messaging Server MIB through two SNMP tables, using a program such as HP OpenView. The tables display both SNMP static variables and MTA variables. For information about these variables, see MIB Variables.

For detailed information about the MIB in SNMP, version 1, see RFC 1212 and RFC 1215.

Note: The Messaging Server MIB supports a subset of the objects defined by the MADMAN MIB, as described in RFC 1566. For further information about this subset, contact the Netscape Server Group.

How the MIB Is Activated

To activate the MIB, you must first install the SNMP master agent for the server and then enable the SNMP subagent, which calls the MIB.

The master agent exchanges information between the network management station (NMS) and its subagents. For more information about the master agent, see the documentation for the Netscape Administration Server.

Once you have installed the master agent, you enable the SNMP subagent. The master agent asks the subagent for information, and the subagent queries the variables defined in the MIB. For more information about the subagent, see The Messaging Server Subagent in Chapter 10.

Format of MIB Entries

The MIB file contains the definitions for managed objects, or variables, that store network information for the server. Each variable definition includes the variable name, its data type and read/write access level, a brief description, and a permanent object identifier. All MIB objects are defined using Abstract Syntax Notation One (ASN.1).

This sample entry shows the definition for the `nsmailEntityDescr` variable:

```
nsmailEntityDescr      OBJECT-TYPE     / object type
           SYNTAX      DisplayString (SIZE (0..255))      / syntax
           ACCESS      read-only      / read/write access level
           STATUS      mandatory      / status
           DESCRIPTION                / description
           "A general textual description of the Netscape Mail Server."
           ::= { nsmailEntityInfo 1 }  / object identifier
```

This definition contains the following information:

- **Object Type** gives the name of the variable, in this case, `nsmailEntityDescr`.
- **Syntax** gives the abstract data type of the variable object type in ASN.1 notation. For example, the Syntax of the `nsmailEntityDescr` variable is `DisplayString (SIZE (0..255))`. See Syntax Types.
- **Access** gives the read/write access level to the variable. Possible access levels are read-only, read-write, write-only, or not-accessible. The access level to all Messaging Server MIB elements is either `read-only`, like that of the `nsmailEntityDescr` variable, or the equivalent `not-accessible`.

- **Status** tells whether the element is mandatory, optional, or obsolete. The Status for all Messaging Server MIB elements is mandatory, or required for the server.
- **Description** is a text description of the element, enclosed in quotes. For example, the description of the `nsmailEntityDescr` variable is "A general textual description of the Netscape Mail Server."
- **Object Identifier** is an assigned name that serves as a permanent identifier for each managed object in the MIB name tree in its namespace. Objects in SNMP are hierarchical; the object identifier is a sequence of labels that represents the object in the hierarchy. For example, `nsmailEntityDescr` is identified as `nsMailEntityInfo 1`. This means that it has the label 1 in the subtree `nsMailEntityInfo`. `nsMailEntityInfo`, in turn, has the label 1 in the `nsmail` subtree.

Syntax Types

The Syntax line of the MIB entry gives the abstract data type of the variable, which must resolve to an instance of an ASN.1 syntax type. These types are defined in various Network Working Group Requests for Comments (RFCs); their definitions are imported into the MIB file, as described in MIB Imports List.

Table D.1 lists the data types used in the Messaging Server MIB, with descriptions, import sources, and examples from the MIB.

Table D.1 Data Types of Messaging Server MIB Variables

Data type	Description and import	Example
`Counter32`	32-bit unsigned long; increases to a maximum value, then restarts from zero. Imported from SNMPv2-SMI.	`mtaReceivedMessages`
`DisplayString`	Human-readable ASCII string with length of 0 to 255 characters. Imported from SNMPv2-TC.	`nsmailEntityDescr`
`Gauge32`	32-bit unsigned long; can increase or decrease between set values. Imported from SNMPv2-SMI.	`mtaStoredMessages`

Table D.1 Data Types of Messaging Server MIB Variables

Data type	Description and import	Example
`INTEGER`	Integer.	`mtaId`
`MtaEntry`	Table format for MTA data retrieval; defines an entry in the `MTAtable`. Defined in the Messaging Server MIB.	`mtaEntry`
`SEQUENCE OF MtaEntry`	Constructor type that generates a table using the specified list constructor; here, it generates the MTA table using the `MtaEntry` type. Defined in ASN.1.	`mtaTable`

Description of the MIB File

The MIB file is organized into several main parts:

- MIB Imports List. The MIB imports list tells the sources of the object and data type definitions used in the MIB.
- Module Definition. The module definition contains organization information and a description of the MIB.
- MIB Variables. MIB variables store the basic information required for network management.
- MIB Traps. A MIB trap is a message sent by the server to alert the NMS about a server event.

MIB Imports List

The Imports list at the beginning of the MIB file gives the sources of the object and data type definitions used in the MIB. For example, the `Counter32` and `Gauge32` data type definitions are imported from the SNMPv2-SMI module. For the text of the import section, see the Imports list in The Messaging Server MIB.

Module Definition

The module definition for the MIB file contains organization information and a description of the MIB. The Messaging Server MIB names the Netscape Communications Corporation as its organization, gives the company name and address as its contact information, and provides a text description of the MIB. For the text of the module definition, see The Messaging Server MIB.

MIB Variables

The MIB defines a number of managed objects, or variables, which have names and values. Variables store information required for network management. You can view the data stored in MIB variables using a program such as HP OpenView.

Messaging Server MIB variables are organized into data for two tables.

- The static variables table provides basic information about the Messaging Server installation. See Static Variables.
- The MTA Table and MTA variables store information specific to the MTA (Message Transfer Agent). See MTA Table for Server Statistics.

Static Variables

The static variables table provides basic information about the Messaging Server installation, such as the version number, the physical location of the server, and contact information. Static variable values are set during server installation and cannot be updated while the server is running.

Table D.2 lists static variables alphabetically by name, with descriptions and examples.

Table D.2 Quick Reference to MIB Attributes: Static Variables

Attribute	Description	Examples
nsmailEntityContact	Contact person for Messaging Server at this installation, usually a server administrator.	John Smith (jsmith@acme.com)
nsmailEntityDescr	Text description of Messaging Server.	Netscape Messaging Server
nsmailEntityLocation	Physical location of Messaging Server, usually a street address.	999 Worldend Rd.
nsmailEntityName	Name assigned to Messaging Server at this installation; should match the link on the Administration Server selection page for Messaging Server.	MTA-40
nsmailEntityOrg	Organization using Messaging Server, usually a department or company name.	Acme Corp.
nsmailEntityVers	Version of Messaging Server that is installed.	4.0

MTA Table for Server Statistics

The MTA Table and MTA variables store information specific to the MTA (Message Transfer Agent), such as the number and volume of messages sent, received, or stored.

The MTA is a program for message routing and delivery. Several MTAs can cooperate in getting messages for the intended recipient. Messages are either delivered to the local message store by the MTA or routed to another MTA for remote delivery.

Table D.3 lists MTA MIB variables alphabetically by name, with descriptions.

Table D.3 Quick Reference to MIB Attributes: MTA Table

Attribute	Description
`mtaId`	Identifier of the MTA for this installation. Since only one Netscape Messaging Server can be installed, this attribute can have only one value.
`mtaReceivedMessages`	Total number of messages received since MTA initialization.
`mtaReceivedRecipients`	Number of recipients for all messages received since MTA initialization.
`mtaReceivedVolume`	Total volume of messages received since MTA initialization, in kilo-octets.
`mtaStoredMessages`	Total number of messages stored in the MTA.
`mtaStoredRecipients`	Number of recipients for all messages stored in the MTA.
`mtaStoredVolume`	Total volume of messages stored in the MTA, in kilo-octets.
`mtaTransmittedMessages`	Total number of messages transmitted since MTA initialization.
`mtaTransmittedRecipients`	Number of recipients specified in all messages transmitted since MTA initialization.
`mtaTransmittedVolume`	Total volume of messages transmitted since MTA initialization, in kilo-octets.

MIB Traps

A MIB trap is a message from the server that notifies the NMS of server events. Messaging Server MIB traps notify the NMS when the server may be down, does not respond to polling, or has restarted.

The SNMP trap is an example of managed device-initiated communication. For more information, see Communication Between the NMS and the Managed Device in Chapter 10.

Each trap sends additional MIB information about the server when it reports an event. The following example shows the information sent with the `nsMailServerDown` trap: Netscape Messaging Server's general description, version number, location, and contact information.

```
nsmailEntityDescr, nsmailEntityVers,
nsmailEntityLocation, nsmailEntityContact
```

Note: To make sure that traps are sent to the NMS, you must set the correct community and trap destination information through the Administration Server. See the documentation for the Administration Server.

Table D.4 lists traps alphabetically by name, with descriptions.

Table D.4 Quick Reference to MIB Attributes: Traps

Trap	Description
`nsMailServerDown`	Messaging Server may be down. Sends general description, version number, location, and contact information for the server at the time of the event.
`nsMailServerNoResponse`	Messaging Server does not respond to its polls, but may still be up and working. Sends general description, version number, location, and contact information for the server at the time of the event.
`nsMailServerStart`	Messaging Server starts or restarts. Sends general description, version number, and location of the server at the time of the event.

The Messaging Server MIB

For your convenience, this section includes the text of the Messaging Server MIB.

```
SNMP MIB


Netscape Messaging Server 4.0
```

```
This file contains Netscape Messaging Server's Simple Network
Management Protocol (SNMP) Management Information Base (MIB).


NSMAIL-MIB DEFINITIONS ::= BEGIN


IMPORTS
           MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY
                     FROM SNMPv2-SMI
           enterprises
                     FROM ObjectIds
           Counter32, Gauge32
                     FROM SNMPv2-SMI
           Counter, IpAddress, TimeTicks
                     FROM RFC1155-SMI
           DisplayString, TimeInterval
                     FROM SNMPv2-TC
           TRAP-TYPE
                     FROM RFC-1215;


           netscape OBJECT IDENTIFIER ::= { enterprises 1450 }


           nsmail MODULE-IDENTITY
           LAST-UPDATED         "9706021700Z"
           ORGANIZATION         "Netscape Communications Corp."
           CONTACT-INFO         "Netscape Communications Corp.
                                 501 E. Middlefield Rd.
                                 Mountain View, CA 94043"

           DESCRIPTION          "A private MIB module for Netscape
                                 Messaging Server"

           ::= { netscape 5 }
```

```
-----
-- Static variables
-----
           nsmailEntityInfo OBJECT IDENTIFIER ::= { nsmail 1 }

           nsmailEntityDescr     OBJECT-TYPE
               SYNTAX     DisplayString (SIZE (0..255))
               ACCESS     read-only
               STATUS     mandatory
               DESCRIPTION   "A general textual description
                              of the Netscape Mail Server."
               ::= { nsmailEntityInfo 1 }

           nsmailEntityVers     OBJECT-TYPE
               SYNTAX     DisplayString (SIZE (0..255))
               ACCESS     read-only
               STATUS     mandatory
               DESCRIPTION  “The Version of the Netscape Mail Server."
               ::= { nsmailEntityInfo 2 }

           nsmailEntityOrg     OBJECT-TYPE
               SYNTAX     DisplayString (SIZE (0..255))
               ACCESS     read-only
               STATUS     mandatory
               DESCRIPTION  "Organization responsible for Netscape
                             Mail Server at this installation."
               ::= { nsmailEntityInfo 3 }

          nsmailEntityLocation     OBJECT-TYPE
             SYNTAX     DisplayString (SIZE (0..255))
             ACCESS     read-only
```

```
                STATUS     mandatory
                DESCRIPTION  "Physical location of this entity
                             (Netscape Mail Server). For example:
                             hostname, building number,
                             lab number, etc."
                  ::= { nsmailEntityInfo 4 }

            nsmailEntityContact     OBJECT-TYPE
                SYNTAX      DisplayString (SIZE (0..255))
                ACCESS      read-only
                STATUS      mandatory
                DESCRIPTION "Contact person(s) responsible for the
                             Netscape Mail Server at this
                             installation, together with
                             information on how to contact."
                 ::= { nsmailEntityInfo 5 }

             nsmailEntityName     OBJECT-TYPE
                 SYNTAX     DisplayString (SIZE (0..255))
                 ACCESS     read-only
                 STATUS     mandatory
                 DESCRIPTION  "Name assigned to this entity at the
                               installation site."
                 ::= { nsmailEntityInfo 6 }

-----
-- mta table for statistic information
-----
           mtaTable       OBJECT-TYPE
               SYNTAX     SEQUENCE OF MtaEntry
               ACCESS     not-accessible
               STATUS     mandatory
```

```
    ::= { nsmail 2 }

mtaEntry       OBJECT-TYPE
    SYNTAX     MtaEntry
    ACCESS     not-accessible
    STATUS     mandatory
    INDEX     { mtaId }
    ::= { mtaTable 1 }

MtaEntry     ::= SEQUENCE {
    mtaReceivedMessages         Counter32,
    mtaStoredMessages           Gauge32,
    mtaTransmittedMessages      Counter32,
    mtaReceivedVolume           Counter32,
    mtaStoredVolume             Gauge32,
    mtaTransmittedVolume        Counter32,
    mtaReceivedRecipients       Counter32,
    mtaStoredRecipients         Gauge32,
    mtaTransmittedRecipients    Counter32,
    mtaId                       INTEGER
    }

mtaReceivedMessages     OBJECT-TYPE
    SYNTAX     Counter32
    ACCESS     read-only
    STATUS     mandatory
    DESCRIPTION  "The total number of messages received
                  since MTA Initialization."
    ::= { mtaEntry 1 }

mtaStoredMessages     OBJECT-TYPE
    SYNTAX     gauge32
```

```
    ACCESS     read-only
    STATUS     mandatory
    DESCRIPTION  "The total number of messages currently
                  stored in the MTA."
    ::= { mtaEntry 2 }

mtaTransmittedMessages     OBJECT-TYPE
    SYNTAX     Counter32
    ACCESS     read-only
    STATUS     mandatory
    DESCRIPTION  "The total number of messages
                  transmitted since MTA Initialization."
    ::= { mtaEntry 3 }

mtaReceivedVolume     OBJECT-TYPE
    SYNTAX     Counter32
    ACCESS     read-only
    STATUS     mandatory
    DESCRIPTION  "The number of msgs (in kilo-octets
                  received since MTA Initialization."
    ::= { mtaEntry 4 }

mtaStoredVolume     OBJECT-TYPE
    SYNTAX     Gauge32
    ACCESS     read-only
    STATUS     mandatory
    DESCRIPTION  "The total number of msgs
                  (in kilo-octets) currently stored
                  in the MTA."
    ::= { mtaEntry 5 }

mtaTransmittedVolume     OBJECT-TYPE
```

```
        SYNTAX     Counter32
        ACCESS     read-only
        STATUS     mandatory
        DESCRIPTION  "Number of msgs, in kilo-octets,
                     transmitted since MTA initialization."
        ::= { mtaEntry 6 }

    mtaReceivedRecipients     OBJECT-TYPE
        SYNTAX     Counter32
        ACCESS     read-only
        STATUS     mandatory
        DESCRIPTION  "The number of recipients specified
                     in all messages received since MTA
                     Initialization. Recipients this MTA
                     had no responsibility for are not counted."
        ::= { mtaEntry 7 }

    mtaStoredRecipients     OBJECT-TYPE
        SYNTAX     Gauge32
        ACCESS     read-only
        STATUS     mandatory
        DESCRIPTION  "The total number of recipients
                     specified in all messages currently
                     stored in the MTA. Recipients this MTA
                     had no responsibility for are not counted."
        ::= { mtaEntry 8 }

    mtaTransmittedRecipients     OBJECT-TYPE
        SYNTAX     Counter32
        ACCESS     read-only
        STATUS     mandatory
        DESCRIPTION  "The number of recipients specified in
```

```
                                all messages transmitted since MTA
                                Initialization. Rexipients this MTA
                                had no responsibility for are not counted."
                    ::= { mtaEntry 9 }

                mtaId           OBJECT-TYPE
                    SYNTAX      INTEGER
                    ACCESS      read-only
                    STATUS      mandatory
                    DESCRIPTION  The id of the MTA as configured."
                    ::= { mtaEntry 10 }

-----
-- Traps
-----
                nsMailServerDown     TRAP-TYPE
                    ENTERPRISE       netscape
                    VARIABLES       { nsmailEntityDescr, nsmailEntityVers,
                                      nsmailEntityLocation,
                                      nsmailEntityContact }
                    DESCRIPTION      This trap is generated whenever the
                                     agent detects the Netscape Mail
                                     Server to be (potentially) Down."
                    ::= 5001

                nsMailServerStart    TRAP-TYPE
                    ENTERPRISE       netscape
                    VARIABLES      { nsmailEntityDescr, nsmailEntityVers,
                                     nsmailEntityLocation }
                    DESCRIPTION     "This trap is generated whenever
                                     the agent detects the Netscape
                                     Mail Server to have (re)started."
```

```
        ::= 5002

    nsMailServerNoResponse  TRAP-TYPE
        ENTERPRISE       netscape
        VARIABLES      { nsmailEntityDescr, nsmailEntityVers,
                         nsmailEntityLocation,
                         nsmailEntityContact }
        DESCRIPTION     "This trap is generated whenever the
                         agent detects the Netscape Mail Server
                         not responding to its polls. This
                         TRAP is different from the
                         'nsMailServerDown' TRAP, as the
                         Netscape Mail Server is still
                         potentially up, serving its main
                         purpose. But, the SNMP data collection
                         entity has most likely gone down."
        ::= 5003

END
```

Copyright © 1998 Netscape Communications Corporation

Glossary

A record — A type of record stored in a DNS server and containing a host name and its associated IP address. A records are used by messaging servers on the Internet to route email. See also **Domain Name System (DNS)** and **MX record**.

access control — A method for controlling access to a server or to folders and files on a server.

access domain — Limits access to certain Messaging Server operations from within a specified domain. For example, an access domain can be used to limit where mail for an account can be collected.

account — Information that defines a specific user or user group. This information includes the user or group name, valid email address or addresses, and how and where email is delivered.

action — A component of a UBE filter; it specifies the action that is to be performed if a match occurs.

address — Information in an email message that determines where and how the message must be sent. Addresses are found both on message headers and on message envelopes.

address handling — The actions performed by the MTA to detect errors in addressing, to rewrite addresses if necessary, and to match addresses to recipients.

addressing protocol — The addressing rules that make email possible. SMTP is the most widely used protocol on the Internet and the protocol supported by the Netscape Messaging Server. Other protocols include X.400 and UUCP (Unix to Unix Copy Protocol).

administrator — A user with administrative privileges for a server or multiple servers. See also **Messaging Server administrator**.

Allow filter — A Messaging Server access-control rule that identifies clients that are to be allowed access to a service such as IMAP, POP, or SMTP. Compare **Deny filter.**

alternate address — A secondary address for an account, generally a variation on the primary address. In some cases it is convenient to have more than one address for a single account.

anonymous access An optional type of access to a server, in which the user named `anonymous` is granted access without need for a password.

attribute An item of information contained in a tag, such as an HTML tag or a Messaging Multiplexor command tag.

AUTH An SMTP command enabling an SMTP client to specify an authentication method to the server, perform an authentication protocol exchange, and, if necessary, negotiate a security layer for subsequent protocol interactions.

authentication 1) The process of proving the identity of a client user to the Netscape Messaging Server. 2)The process of proving the identity of the Netscape Message Server to a client or another server.

authentication certificate A digital file sent from server to client or client to server to verify and authenticate the other party. The certificate ensures the authenticity of its holder (the client or server). Certificates are not transferable.

AutoReply utility A utility that automatically responds to messages sent to accounts with the AutoReply feature activated. Every account in the Netscape Messaging Server can be configured to automatically reply to incoming messages.

backside port The port that the Messaging Multiplexor uses to communicate with the servers that contain the Multiplexor's clients' mailboxes. Compare **listen port.**

banner A text string displayed by a service such as IMAP when a client first connects to it.

base DN A distinguished name entry in the directory from which searches will occur. Also known as a search base. For example, ou=people, o=airius.com.

bind DN A distinguished name used to authenticate to the Directory Server when performing an operation.

body The main part of an email message. Although headers and envelopes must follow a standard format, the body of the message has a content determined by the sender—the body can contain text, graphics, or even multimedia.

capability A string, provided to clients, that defines the functionality available in a given IMAP service.

case tag A tag in the Message Field component of a UBE filter that specifies that matching should be case-sensitive.

certificate-based authentication Identification of a user from a digital certificate submitted by the client. Compare **password authentication.**

certificate database — A file that contains a server's digital certificate(s). Also called a *cert file*.

certificate name — The name that identifies a certificate and its owner.

cipher — An algorithm used in encryption.

client — A software entity that requests services or information from a server. Compare **user.**

CNAME record — A type of record stored in a DNS server. A CNAME record maps a domain name alias to a domain name.

command tag — A tag that appears in the `mailmaster` commands file; it defines actions to be performed by the Mailstone program.

comment character — A character that, when placed at the beginning of a line, turns the line into a nonexecutable comment. For Netscape configuration files, it is the pound sign (#).

config_util — A command line utility for making changes to configuration information stored in the directory server or in the local configuration file.

counter_util — A command line utility for displaying all counters in a counter object.

daemon — A Unix program that runs in the background, independent of a terminal, and performs a function whenever necessary. Common examples of daemon programs are mail handlers, license servers, and print daemons. On Windows NT machines, this type of program is called a service. See also **service**.

default log — A Messaging Server log file that is produced by a service or utility other than the principal services Administration, SMTP, IMAP, and POP.

Deny filter — A Messaging Server access-control rule that identifies clients that are to be denied access to a service such as IMAP, POP, or SMTP. Compare **Allow filter.**

deliver — A command line utility for delivering mail to POP or IMAP folders.

directive — An instruction between the opening and closing tags of a pair, such as a pair of HTML tags or a pair of command tags in the Mailstone utility's commands file.

directory lookup — The process of searching the directory for information on a given user or resource, based on that user or resource's name or other characteristic.

directory service — An application designed to manage information about people and resources within an organization. See also **Lightweight Directory Access Protocol**.

DNS See **Domain Name System**.

DNS alias A host name that the DNS server recognizes as pointing to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, `www.airius.domain` might be an alias that points to a real machine called `realthing.airius.domain` where the server currently exists.

DNS spoofing A form of network attack in which a client attempting to access or send a message to a server misrepresents its host name.

domain name A unique name that defines an administrative organization. Domains can contain other domains. Domain names are interpreted from right to left. For example, `airius.com` is both the domain name of the Airius Company and a subdomain of the top-level `com` domain. The `airius.com` domain can be further divided into subdomains such as `corp.airius.com`, and so on. See also **host name** and **fully-qualified domain name**.

Domain Name System (DNS) The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with host names (such as `www.airius.com`). Machines normally get this information from a DNS server. See also **A record** and **MX record**.

domain part The part of an email address that identifies the administrative authority responsible for the recipient.

encryption The process of disguising information so that it cannot be deciphered (decrypted) by anyone but the intended recipient.

enterprise network A network that consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and is used by the company's mission-critical applications.

entry (1) In a directory, the collected information about a single person to resource. (2) In a log file, a line that represents one logged event.

envelope A container for information about the sender and the recipient of an email message. This information is not part of the message header. Envelopes are used by various email programs as messages are moved from place to place. Users see only the header and body of a message.

envelope field A named item of information, such as `RCPT TO`, in a message envelope.

envonly tag A tag in the Message Field component of a UBE filter that restricts the filter processing to the message envelope alone.

error handler A program that handles errors. In the Messaging Server, issues error messages and processes error action forms after the postmaster fills them out.

Error-Handler Action form A form sent to the postmaster account that accompanies a received message that the Messaging Server cannot handle. The postmaster fills out the form to instruct the server how to process the message.

error message A message reporting an error or other situation. Netscape Messaging Server generates messages in a number of situations, notably when it gets an email message that it can't handle. Others messages, called notification errors, are for informational purposes only.

ETRN An SMTP command enabling a client to request that the server start the processing of its mail queues for messages that are waiting at the server for the client machine. Defined in RFC 1985.

EXPN An SMTP command for expanding a mailing list. Defined in RFC 821.

extension library A shared library used to extend or override the capabilities of a plugin such as the UBE plugin.

extranet The part of a company intranet that customers and suppliers can access. See also **intranet**.

facility In a Messaging Server log-file entry, a designation of the software subsystem (such as Network or Account) that generated the log entry.

filter See **UBE filter, Allow filter, Deny filter**.

filter.cfg The file that holds all the UBE filter rules; used by the UBE plugin.

filter.opt A file that controls certain aspects of the behavior of the UBE plugin.

firewall A network configuration, usually both hardware and software, that forms a barrier between networked computers within an organization and those outside the organization. A firewall is commonly used to protect information such as a network's email, discussion groups, and data files within a physical building or organization site.

folder A named collection of messages. Folders can contain other folders. See also **personal folder** and **shared folder**.

forwarding The act that occurs when an MTA sends a message delivered to a particular account to one or more new destinations as specified by the account's attributes. Forwarding may be configurable by the user. See also **routing**.

FQDN See **fully-qualified domain name**.

fully-qualified domain name (FQDN) The unique name that identifies a specific Internet location. See also **domain name**.

greeting form A message usually sent to users when an account is created for them. This form acts as confirmation of the new account and verification of its contents. The greeting form also instructs users on how to change information related to their mail account. During installation, system administrators have the option of deciding whether to send greeting forms to users.

hashdir A command line utility for determining which directory contains the message store for a particular user.

header The portion of an email message that precedes the body of the message. Headers contain information useful to email programs and to users trying to make sense of the message: they tell whom the message is for, who sent it, when it was sent, and what it is about. Headers must be written according to the SMTP protocol so that email programs can read them.

header field A named item of information, such as `From:` or `To:`, in a message header.

hop A transmission between two computers.

host The machine on which one or more servers reside.

host name The name of a particular machine within a domain. The fully qualified host name consists of two parts: the host name and the domain name. For example, `mail.airius.com` is the machine `mail` in the domain `airius.com`. Host names must be unique within their domains. Your organization can have multiple machines named `mail`, as long as the machines reside in different subdomains; for example, `mail.corp.airius.com` and `mail.field.airius.com`. Host names always map to a specific IP address. See also **domain name**, **fully-qualified domain name**, and **IP address**.

host name hiding The practice of having domain-based email addresses that don't contain the name of a particular host.

hub A host that acts as the single point of contact for the system. When two networks are separated by a firewall, for example, the firewall computer often acts as a mail hub.

IMAP4 See **Internet Message Access Protocol Version 4**.

ImapMMP.config A configuration file that defines an IMAP4 instance of the Messaging Multiplexor.

ImapMMP.sh A Unix shell script that sets configuration parameters and executes the IMAP Messaging Multiplexor.

ImapProxy The executable file for the IMAP Messaging Multiplexor.

imscripter A command line utility that talks to an IMAP server. You can use this utility to execute a command or batch of commands on IMAP folders.

installation directory The directory into which the binary (executable) files of a server are installed. For the Messaging Server, it is a subdirectory of the server root: *`serverRoot`*`/bin/msg/`. Compare **instance directory**, **server root**.

instance A separately executable configuration of a server or other software entity on a given host. With a single installed set of binary files, it is possible to create multiple instances of Netscape servers that can be run and accessed independently of each other.

instance directory The directory that contains the files that define a specific instance of a server. For the Messaging Server, it is a subdirectory of the server root: *`serverRoot`*`/msg-`*`instanceName`*`/`, where *`instanceName`* is the name of the server as specified at installation. Compare **installation directory**, **server root**.

Internet The name given to the worldwide network of networks that uses TCP/IP protocols.

Internet Message Access Protocol Version 4 (IMAP4) A standard protocol that allows users to be disconnected from the main messaging system and still be able to process their mail. The IMAP specification allows for administrative control for these disconnected users and for the resynchronization of the users' message store once they reconnect to the messaging system.

Internet Protocol (IP) The basic network-layer protocol on which the Internet and intranets are based.

intranet A network of TCP/IP networks within a company or organization. Intranets enable companies to employ the same types of servers and client software used for the World Wide Web for internal applications distributed over the corporate LAN. Sensitive information on an intranet that communicates with the Internet is usually protected by a firewall. See also **firewall** and **extranet**.

IP See **Internet Protocol**.

IP address A set of numbers, separated by dots, such as `198.93.93.10`, that specifies the actual location of a machine on an intranet or the Internet.

key database A file that contains the key pair(s) for a server's certificate(s). Also called a key file.

label A component of a UBE filter; it provides a named destination for the actions of other filters.

LDAP See **Lightweight Directory Access Protocol**.

LDAP Data Interchange Format (LDIF) The format used to represent Directory Server entries in text form.

LDAP search string A string with replaceable parameters that defines the attributes used for directory searches. For example, an LDAP search string of `"uid=%s"` means that searches are based on the user ID attribute.

LDIF See **LDAP Data Interchange Format**.

level A designation of logging verbosity, meaning the relative number of types of events that are recorded in log files. At a level of Emergency, for example, very few events are logged; at a level of Informational, on the other hand, very many events are logged.

Lightweight Directory Access Protocol (LDAP) Directory service protocol designed to run over TCP/IP and across multiple platforms. A simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of user and group account management across Netscape servers. The Netscape Directory Server uses the LDAP protocol.

listen port The port that a server uses to communicate with clients and other servers. The Messaging Multiplexor can use both a listen port and a separate backside port.

local part The part of an email address that identifies the recipient. See also **domain part**.

log directory The directory in which all of a service's log files are kept.

log expiration Deletion of a log file from the log directory after it has reached its maximum permitted age.

log rotation Creation of a new log file to be the current log file. All subsequent logged events are to be written to the new current file. The log file that was the previous current file is no longer written to, but remains in the log directory.

mailbox See **folder**.

mail client The programs that help users send and receive email. This is the part of the various networks and mail programs that users have the most contact with. Mail clients create and submit messages for delivery, check for new incoming mail, and accept and organize incoming mail.

mailclient The main program used by the Mailstone utility.

mailclient commands file A configuration file that defines the commands to be executed by the Mailstone utility.

mail exchange record See **MX record**.

mailmaster A Perl script used by the Mailstone utility to control execution of the `mailclient` program on multiple client hosts.

mailmaster client The client machine on which the `mailmaster` script executes in a Mailstone test configuration.

mailmaster configuration file A file that defines test parameters for the Mailstone utility.

Mailstone A utility for performing stress tests. The Mailstone utility enables you to perform capacity planning by testing the ability of your mail server to function properly under maximum loads.

Management Information Base (MIB) A database containing data about managed network objects.

master agent The SNMP agent that exchanges information between the Network Management station (NMS) and its subagents. See also **subagent**.

match criterion A component of a UBE filter; it is a string or expression that represents an envelope or header phrase (such as `"Easy Money"`) to be matched against incoming messages.

mboxutil A command line utility for managing mail folders.

MD5 A message digest algorithm by RSA Data Security. MD5 can be used to produce a short digest of data that is unique with high probability. It is mathematically extremely hard to produce a piece of data that produces the same message digest email.

message The fundamental unit of email, a message consists of a header and a body and is often contained in an envelope while it is in transit from the sender to the recipient.

message delivery When the MTA delivers a message to a local recipient (a mail folder or a program).

message field A component of a UBE filter; it specifies the specific envelope or header item (such as `Subject:`) whose contents are to be matched against incoming messages.

Message Handling System (MHS) A group of connected MTAs, their user agents, and message stores.

message queue The directory where messages accepted from clients and other mail servers are queued for delivery (immediate or deferred).

message quota A limit defining how much disk space a particular folder can consume.

message store The database of all locally delivered messages for a Messaging server instance. Messages can be stored on a single physical disk or stored across multiple physical disks.

message store partition A message store or subset of a message store residing on a single physical file system partition.

Message Transfer Agent (MTA) A specialized program for routing and delivering messages. MTAs work together to transfer messages and deliver them to the intended recipient. The MTA determines whether a message is delivered to the local message store or routed to another MTA for remote delivery.

Messaging Multiplexor A specialized Netscape Messaging Server that acts as a single point of connection to multiple mail servers, facilitating the distribution of a large user base across multiple mailbox hosts.

Messaging Server administrator The administrator whose privileges include installation and administration of a Netscape Messaging Server instance.

MHS See **Message Handling System**.

MIB See **Management Information Base**.

MIME See **Multipurpose Internet Mail Extension**.

mmp-setup The Unix filename for the Messaging Multiplexor installer.

MoveUser A command line utility for moving messages in a user's mail folder from one Messaging Server to another.

msgalarmproc A command line utility for monitoring disk usage and server response time.

MTA See **Message Transfer Agent**.

MTA hop The act of routing a message from one MTA to another.

Multiplexor See **Messaging Multiplexor**.

Multipurpose Internet Mail Extension (MIME) A protocol you can use to include multimedia in email messages by appending the multimedia file in the message. Because not all mail clients support MIME, you should make sure that the message recipient has a MIME-enabled mail client.

MX record A type of record stored in a DNS server that maps a domain name to a host name.

net mask A 32-bit value used in conjunction with an IP address to separate the network and subnet IDs from the host ID.

Netscape administrator The administrator whose privileges include installation and administration of all Netscape servers, including the Netscape Directory Server.

Netscape Console The administrator interface from which you administer all Netscape servers.

Netscape Setup The installation program for all Netscape servers and for Netscape Console.

next-hop list A list of adjacent systems a mail route uses to determine where to transfer a message. The order of the systems in the next-hop list determines the order in which the mail route transfers messages to those systems.

notification message A type of message, sent to the postmaster account by the Messaging Server, that is for information al purposes and requires no action from the postmaster. Compare **error message.**

NscpMsg (Unix only) A command line utility for starting and stopping the Netscape Messaging Server and for running recovery utilities.

nsfilter The shared library file that contains the UBE plugin.

partition See **message store partition**.

password authentication Identification of a user through user name and password. Compare **certificate-based authentication.**

pattern A string expression used for matching purposes, such as in Allow and Deny filters.

personal folder A folder that can be read only by the owner. See also **shared folder**.

plain text authentication See **password authentication.**

plugin A server extension program, implemented on the Messaging Server as a shared library that uses the Messaging Server Plugin API.

POP3 See **Post Office Protocol Version 3**.

PopMMP.config A configuration file that defines a POP3 instance of the Messaging Multiplexor.

PopMMP.sh A Unix shell script that sets configuration parameters and executes the POP3 Messaging Multiplexor.

PopProxy The executable file for the POP Messaging Multiplexor.

port number A number that specifies an individual TCP/IP application on a host machine, providing a destination for transmitted data.

postmaster By convention, an account used to communicate with the person (or people) responsible for maintaining a messaging server.

Post Office Protocol Version 3 (POP3) A protocol that provides a standard delivery method and that does not require the message transfer agent to have access to the user's mail folders. Not requiring access is an advantage in a networked environment, where often the mail client and the message transfer agent are on different computers.

process A self-contained, fully functional execution environment set up by an operating system. Each instance of an application typically runs in a separate process. Compare **thread.**

qconvert A command line utility for converting the Netscape Messaging Server 3.x message queue to the 4.0 MTA format.

quota A command line utility for viewing reports about and fixing message quota usage. See also **message quota**.

RC2 A variable key-size block cipher by RSA Data Security.

RC4 A stream cipher by RSA Data Security. Faster than RC2.

readership A command line utility for collecting readership information on mail folders.

reconstruct A command line utility for reconstructing mail folders.

regular expression A text string that uses special characters to represent ranges or classes of characters for the purpose of pattern matching.

routing The act of transferring a message from one MTA to another when the first MTA determines that the recipient is not a local account, but might exist elsewhere. Routing is normally configurable only by a network administrator. See also **forwarding**.

routing tables The internal databases that hold the information about message originators and recipients. See also **SMTP mail routing table**.

RUN action A special action of the UBE plugin; it calls external programs that extend the plugin.

schema Definitions of the types of information that can be stored as entries in the Netscape Directory Server. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

search base See **base DN**.

Secure Sockets Layer (SSL) A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

security-module database A file that contains information describing hardware accelerators for SSL ciphers. Also called *secmod*.

sendmail A common MTA used on Unix machines. In most applications, the Netscape Messaging Server can be used as a dropin replacement for sendmail. Netscape provides a set of sendmail migrations tools.

server instance The directories, programs, and utilities representing a specific server installation.

server root The directory into which all Netscape servers associated with a given Administration Server on a given host are installed. Typically designated *`serverRoot`*. Compare **installation directory**, **instance directory**.

service (1) A background process on Windows NT that does not have a user interface. Netscape servers on Windows NT platforms run as services. Equivalent to **daemon.** (2) A function provided by a server. For example, the Netscape Messaging Server provides IMAP, POP, and SMTP services.

session An instance of a client-server connection.

shared folder A folder that can be read by more than one person. Compare **personal folder**.

Simple Mail Transfer Protocol (SMTP) The email protocol most commonly used by the Internet and the protocol supported by the Netscape Messaging Server.

Simple Network Management Protocol (SNMP) A network protocol that allows administrators to monitor server processes remotely on SNMP-compatible servers through the use of SNMP station software.

SIZE An SMTP command enabling a client to declare the size of a particular message to a server. The server may indicate to the client that it is or is not willing to accept the message based on the declared message size; the server can declare the maximum message size it is willing to accept to a client. Defined in RFC 1870.

SMTP See **Simple Mail Transfer Protocol**.

smtpAccept The stage of SMTP message processing that involves accepting messages sent from clients or other servers.

smtpDeliver The stage of SMTP message processing that involves transferring messages to other servers.

SMTP mail routing table Provides a way to redirect mail based on the domain to which it is being sent. Each entry in the SMTP Mail Routing table consists of a pattern and a domain. Before sending a message, the destination domain is compared to the patterns in the table. If a match is found, the destination host is replaced by the domain corresponding to the pattern that matched.

SNMP See **Simple Network Management Protocol**.

spoof message A message that the Messaging Multiplexor can send to a user when the Multiplexor cannot connect to the user's mailbox server.

spoofing Misrepresentation of its host name, domain name, or IP address by a client attempting to gain access to or send a message to a server.

SSL See **Secure Sockets Layer**.

subagent An SNMP agent that gathers information regarding network activity of a particular device, such as the Netscape Messaging Server.

subdomain A portion of a domain. For example, in the domain name corp.airius.com, corp is a subdomain of the domain airius.com. See also **host name** and **fully-qualified domain name.**

subnet The portion of an IP address that identifies a block of host IDs.

TCP See **Transmission Control Protocol**.

TCP/IP See **Transmission Control Protocol/Internet Protocol**.

thread A lightweight execution instance within a process.

Transmission Control Protocol (TCP) The basic transport protocol in the Internet protocol suite that provides reliable, connection-oriented stream service between two hosts.

Transmission Control Protocol/ Internet Protocol (TCP/IP) The name given to the collection of network protocols used by the Internet protocol suite. The name refers to the two primary network protocols of the suite: TCP (Transmission Control Protocol), the transport layer protocol, and IP (Internet Protocol), the network layer protocol.

UA See **user agent**.

UBE See **Unsolicited Bulk Email**.

UBE filter A rule that defines how messages that fit a certain match criterion are to be handled. See also **Unsolicited Bulk Email (UBE).**

UBE plugin An SMTP plugin that applies UBE filters to incoming messages.

Unsolicited Bulk Email (UBE) Unrequested and unwanted email, sent from bulk distributors, usually for commercial purposes.

user (1) A person that makes use of computer software. (2) An account for accessing a server, maintained as an entry on a directory server.

user agent (UA) The client component, such as Netscape Communicator, that allows users to create, send, and receive mail messages.

virtual domain A domain name added by the Messaging Multiplexor to a client's user ID for LDAP searching and for logging into a mailbox server.

VRFY SMTP command for verifying a user name. Defined in RFC 821.

wildcard A special character in a search string that can represent one or more other characters or ranges of characters.

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V