
Mac OS X Server
Mail Service Administration
For Version 10.5 Leopard

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

019-0934/2007-09-01

Contents

Preface 7 **About This Guide**
7 What's New in Version 10.5
7 What's in This Guide
7 Using This Guide
8 Setting Up Mac OS X Server for the First Time
8 Getting Help for Everyday Management Tasks
8 Using Onscreen Help
9 Mac OS X Server Administration Guides
10 Viewing PDF Guides Onscreen
10 Printing PDF Guides
11 Getting Documentation Updates
11 Getting Additional Information

Chapter 1 13 **Mail Service Setup**
14 Mail Service Protocols
14 Outgoing Mail
14 Incoming Mail
16 User Interaction with Mail Service
16 Where Mail Is Stored
16 Outgoing Mail Location
16 Incoming Mail Location
17 Maximum Number of Mail Messages Per Volume
17 Using Web Service with Mail
18 Using Network Services with Mail Service
19 Configuring DNS for Mail Service
19 How Mail Service Uses SSL
20 Enabling Secure Mail Transport with SSL
20 Before You Begin
21 How User Account Settings Affect Mail Service
21 Moving Mail Messages from Apple Mail Server to Mac OS X Server v10.5
21 Overview of Mail Service Tools
21 Setup Overview
22 Configuring Mail Using Server Admin

24 Configuring Incoming Mail Service
24 Enabling POP Access
25 Enabling IMAP Access
25 Choosing No Incoming Mail Retrieval
26 Enabling Secure POP Authentication
26 Enabling Less Secure Authentication for POP
27 Configuring SSL Transport for POP Connections
27 Enabling Secure IMAP Authentication
28 Enabling Less Secure IMAP Authentication
28 Configuring SSL Transport for IMAP Connections
29 Configuring Outgoing Mail Service
29 Enabling SMTP Access
29 Understanding SMTP Authentication
30 Enabling Secure SMTP Authentication
31 Enabling Less Secure SMTP Authentication
31 Configuring SSL Transport for SMTP Connections
32 Relaying SMTP Mail Through Another Server
32 Limiting Incoming Message Size
33 Using ACLs for Mail Service Access
34 Supporting Mail Users
34 Configuring Mail Settings for User Accounts
34 Configuring Mail Client Software
35 Creating an Administration Account
35 Creating Additional Mail Addresses for a User
37 Setting Up Forwarding Mail Addresses for a User
38 Enabling Virtual Hosting
38 Adding or Removing Virtual Hosts
39 Associating Users to the Virtual Host
41 Managing Mail Quotas
41 Enabling Mail Quotas for Users
42 Configuring Quota Warnings
42 Configure Quota Violation Responses
43 Limiting Junk Mail and Viruses
43 Connection Control
46 Filtering SMTP Connections
47 Mail Screening
50 Advanced Configuration Tools and Options
51 cyradm
51 Sieve Scripting Support
54 Configuring Additional Mail Service Support for 8-Bit MIME

Chapter 2 55 **Mail Service Maintenance**
55 Starting and Stopping Mail Service

56 Holding Outbound Mail
56 Blocking Inbound Mail Connections
56 Reloading Mail Service
57 Changing Protocol Settings for Incoming Mail
57 Improving Performance
57 Working with the Mail Store and Database
58 Viewing the Location for the Mail Database and Mail Store
58 Repairing the Mail Database
58 Repairing the Mail User's Account Database
59 Converting the Mail Store and Database from an Earlier Version
59 Specifying the Location of the Mail Database and Mail Store
60 Creating Additional Mail Store Locations
61 Backing Up and Restoring Mail Messages
62 Setting Up Mail Server Clustering
62 Monitoring Mail Messages and Folders
62 Allowing Administrator Access to Mail Folders
63 Saving Mail Messages for Monitoring and Archival Purposes
64 Monitoring Mail Service
64 Viewing Mail Service Activity
64 Viewing the Mail Connections List
64 Checking the Outgoing Mail Queue
65 Clearing Messages from the Outgoing Mail Queue
65 Viewing Mail Accounts
65 Viewing Mail Service Logs
66 Setting Mail Service Log Detail Level
66 Archiving Mail Service Logs by Schedule
67 Reclaiming Disk Space Used by Mail Service Log Archives
67 When a Disk Is Full
67 When Mail Is Undeliverable
67 Forwarding Undeliverable Incoming Mail
68 Copying Undeliverable Incoming Mail
68 Retrying Undelivered Outgoing Messages
69 Where to Find More Information
69 Books
69 Internet

Chapter 3 71 **Mailing Lists**
72 Setting Up a Groups-based Mailing List
73 Setting Up a Mailman Mailing List
73 Enabling Mailing Lists
74 Creating a Mailing List
75 Setting a List's Maximum Message Length
75 Creating a Mailing List Description

76 Customizing the Mailing List Welcome Message
76 Customizing the Mailing List Unsubscribe Message
77 Enabling a Mailing List Moderator
77 Setting Mailing List Message Bounce Options
78 Designating a Mailing List as Private
78 Adding Subscribers
79 Administering Mailing Lists
80 Viewing a Server's Mailing Lists
80 Viewing a Mailing List's Information Page
80 Designating a List Administrator
81 Accessing Web-based Administrator Options
81 Designating a List Moderator
82 Archiving a List's Mail
82 Viewing Mailing List Archives
82 Working with Mailing List Subscribers
83 Adding a Subscriber to a List
83 Removing a List Subscriber
83 Changing Subscribers Posting Privileges
84 Suspending a Subscriber
84 List Subscriber Options
84 Subscribing to a Mailing List Via Mail
85 Subscribing to a Mailing List Via Web
85 Unsubscribing from a Mailing List Via Mail
86 Unsubscribing from a Mailing List Via Web
86 Setting and Changing Your Mailing List Password
87 Disabling List Mail Delivery
87 Changing Digest Mode
88 Choosing MIME or Plain Text Digests
88 Setting Additional Subscriber Options
89 Where to Find More Information

Glossary 91

Index 101

About This Guide

What's New in Version 10.5

Mac OS X Server's Mail service includes the following new features:

- New failover and cluster administration for Xsan installations
- Automatic group mailing addresses for workgroups defined in Open Directory

What's in This Guide

This guide is organized into three chapters:

- Chapter 1, "Mail Service Setup," on page 13, includes everything you need to set up and configure mail service and to support and configure mail users.
- Chapter 2, "Mail Service Maintenance," on page 55, includes information for ongoing mail server maintenance and administration.
- Chapter 3, "Mailing Lists," on page 71, explains the mailing list service in Mac OS X Server. Mailing lists are a powerful collaboration tool for disseminating and archiving mail discussions.

In addition, the Glossary provides brief definitions of the terms used in this guide.

Using This Guide

The first chapter provides an overview of how Mail service works, what it can do for you, strategies for using it, how to set it up for the first time, and how to administer it over time.

Also take a look at any chapter that describes a service you're unfamiliar with. You may find that some of the services you haven't used before can help you run your network more efficiently and improve performance for your users.

Most chapters end with a section called "Where to Find More Information." This section points you to websites and other reference material containing more information about the service.

Setting Up Mac OS X Server for the First Time

If you haven't installed and set up Mac OS X Server, do so now.

- For instructions on server installation and setup, refer to *Getting Started* , the document that came with your software. For many environments, this document provides all the information you need to get your server up and running and available for initial use.
- Read specific sections to learn how to continue setting up individual features of mail service. Pay particular attention to the information in these sections: "Setup Overview," and "Before You Begin."

Getting Help for Everyday Management Tasks

If you want to change settings, monitor services, view service logs, or do any other day-to-day administration task, you can find step-by-step procedures by using the onscreen help available within Mac OS X Server.

All administration tasks are documented in the second chapter of this guide, but it may be more convenient to retrieve information from onscreen help while using your server.

Using Onscreen Help

You can get task instructions onscreen in the Help Viewer application while you're managing Leopard Server. You can view help on a server or an administrator computer. (An administrator computer is a Mac OS X computer with Leopard Server administration software installed on it.)

To get help for an advanced configuration of Leopard Server:

- Open Server Admin or Workgroup Manager and then:
  - Use the Help menu to search for a task you want to perform.
  - Choose Help > Server Admin Help or Help > Workgroup Manager Help to browse and search the help topics.

The onscreen help contains instructions taken from *Server Administration* and other advanced administration guides described in "Mac OS X Server Administration Guides," next.

To see the most recent server help topics:

- Make sure the server or administrator computer is connected to the Internet while you're getting help.

  Help Viewer retrieves and caches the most recent server help topics from the Internet. When not connected to the Internet, Help Viewer displays cached help topics.

Mac OS X Server Administration Guides

Getting Started covers installation and setup for standard and workgroup configurations of Mac OS X Server. For advanced configurations, *Server Administration* covers planning, installation, setup, and general server administration. A suite of additional guides, listed below, covers advanced planning, setup, and management of individual services. You can get these guides in PDF format from the Mac OS X Server documentation website:

www.apple.com/server/documentation

This guide...	tells you how to:
Getting Started and *Mac OS X Server Worksheet*	Install Mac OS X Server and set it up for the first time.
Command-Line Administration	Install, set up, and manage Mac OS X Server using UNIX command-line tools and configuration files.
File Services Administration	Share selected server volumes or folders among server clients using the AFP, NFS, FTP, and SMB protocols.
iCal Service Administration	Set up and manage iCal shared calendar service.
iChat Service Administration	Set up and manage iChat instant messaging service.
Mac OS X Security Configuration	Make Mac OS X computers (clients) more secure, as required by enterprise and government customers.
Mac OS X Server Security Configuration	Make Mail service and the computer it's installed on more secure, as required by enterprise and government customers.
Mail Service Administration	Set up and manage IMAP, POP, and SMTP mail services on the server.
Network Services Administration	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, NAT, and RADIUS services on the server.
Open Directory Administration	Set up and manage directory and authentication services, and configure clients to access directory services.
Podcast Producer Administration	Set up and manage Podcast Producer service to record, process, and distribute podcasts.
Print Service Administration	Host shared printers and manage their associated queues and print jobs.
QuickTime Streaming and Broadcasting Administration	Capture and encode QuickTime content. Set up and manage QuickTime streaming service to deliver media streams live or on demand.
Server Administration	Perform advanced installation and setup of server software, and manage options that apply to multiple services or to the server as a whole.
System Imaging and Software Update Administration	Use NetBoot, NetInstall, and Software Update to automate the management of operating system and other software used by client computers.
Upgrading and Migrating	Use data and service settings from an earlier version of Mail Service or Windows NT.

This guide...	tells you how to:
User Management	Create and manage user accounts, groups, and computers. Set up managed preferences for Mac OS X clients.
Web Technologies Administration	Set up and manage web technologies, including web, blog, webmail, wiki, MySQL, PHP, Ruby on Rails, and WebDAV.
Xgrid Administration	Set up and manage computational clusters of Xserve systems and Mac computers.
Mac OS X Server Glossary	Learn about terms used for server and storage products.

Viewing PDF Guides Onscreen

While reading the PDF version of a guide onscreen:

- Show bookmarks to see the guide's outline, and click a bookmark to jump to the corresponding section.
- Search for a word or phrase to see a list of places where it appears in the document. Click a listed place to see the page where it occurs.
- Click a cross-reference to jump to the referenced section. Click a web link to visit the website in your browser.

Printing PDF Guides

If you want to print a guide, you can take these steps to save paper and ink:

- Save ink or toner by not printing the cover page.
- Save color ink on a color printer by looking in the panes of the Print dialog for an option to print in grays or black and white.
- Reduce the bulk of the printed document and save paper by printing more than one page per sheet of paper. In the Print dialog, change Scale to 115% (155% for *Getting Started*). Then choose Layout from the untitled pop-up menu. If your printer supports two-sided (duplex) printing, select one of the Two-Sided options. Otherwise, choose 2 from the Pages per Sheet pop-up menu, and optionally choose Single Hairline from the Border menu. (If you're using Mac OS X v10.4 or earlier, the Scale setting is in the Page Setup dialog and the Layout settings are in the Print dialog.)

You may want to enlarge the printed pages even if you don't print double sided, because the PDF page size is smaller than standard printer paper. In the Print dialog or Page Setup dialog, try changing Scale to 115% (155% for *Getting Started*, which has CD-size pages).

Getting Documentation Updates

Periodically, Apple posts revised help pages and new editions of guides. Some revised help pages update the latest editions of the guides.

- To view new onscreen help topics for a server application, make sure your server or administrator computer is connected to the Internet and click "Latest help topics" or "Staying current" in the main help page for the application.
- To download the latest guides in PDF format, go to the Mac OS X Server documentation website:

  www.apple.com/server/documentation

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx)—gateway to extensive product and technology information.
- *Mail Service Support website* (www.apple.com/support/macosxserver)—access to hundreds of articles from Apple's support organization.
- *Apple Training website* (www.apple.com/training)—instructor-led and self-paced courses for honing your server administration skills.
- *Apple Discussions website* (discussions.apple.com)—a way to share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using mail.

Mail Service Setup

1

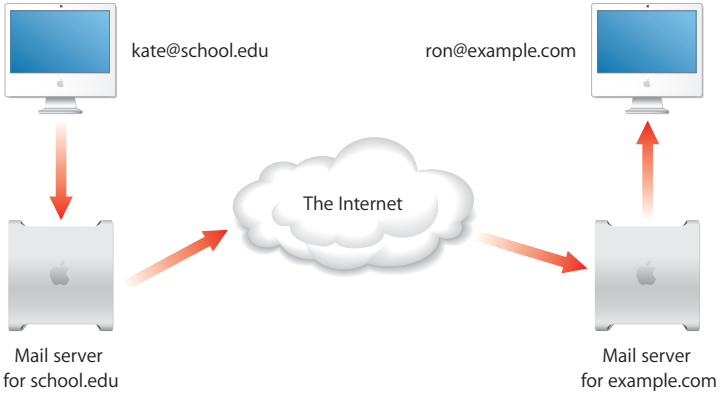
Mail service in Mac OS X Server allows network users to send and receive mail over your network or across the Internet.

Mail service sends and receives mail using the following standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP).

Mail service also uses a Domain Name System (DNS) service to determine the destination IP address of outgoing mail.

This chapter begins with a look at the standard protocols used for sending and receiving mail. Then it explains how Mail service works, summarizes the aspects of Mail service setup, and tells you how to:

- Set up Mail service for incoming and outgoing mail
- Support mail users
- Limit junk mail



Mail Service Protocols

A standard mail client setup uses SMTP to send outgoing mail, and POP and IMAP to receive incoming mail. Mac OS X Server includes an SMTP service and a combined POP and IMAP service. You may find it helpful to take a closer look at these mail protocols.

Outgoing Mail

Outgoing mail service is the means by which users can send mail across the Internet. Subject to restrictions you specify, the SMTP service also transfers mail to and from mail services on other servers.

If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service.

Simple Mail Transfer Protocol (SMTP)

SMTP is a protocol used to send and transfer mail. SMTP queues outgoing mail messages from the user. These messages are transferred over the Internet to their destinations, to be picked up by incoming mail protocols.

Mac OS X Server uses Postfix as its mail transfer agent (MTA). Postfix fully supports SMTP. Your mail users will set their mail application's outgoing mail server to your Mac OS X Server running Postfix, and access incoming mail from a Mac OS X Server running incoming mail service.

More information about Postfix can be found at: www.postfix.org

If you use another MTA (such as Sendmail), you can't configure your mail service with Mac OS X Server administration tools.

To use Sendmail instead of Postfix, you must disable the current SMTP service through Postfix, then install and configure Sendmail. For more information about Sendmail, see www.sendmail.org.

Incoming Mail

Mail is transferred from incoming mail storage to the mail recipient's inbox by a local delivery agent (LDA). The LDA handles local delivery, making mail accessible by the user's mail application. Two protocols are available from Mac OS X Server's mail access agent: POP and IMAP.

Mac OS X Server uses Cyrus to provide POP and IMAP service. More information about Cyrus can be found at: asg.web.cmu.edu/cyrus

Post Office Protocol (POP)

POP is used only for receiving mail, not for sending mail.

The POP service is like a post office, storing mail and delivering it to a specific address. Mail service stores incoming POP mail until users connect to the Mail service and download their waiting mail.

After a user's computer downloads POP mail, the mail is stored only on the user's computer. The user's computer disconnects from Mail service, and the user can read, organize, and reply to the received POP mail.

An advantage of using POP is that your server doesn't need to store mail that users have downloaded. Therefore, your server doesn't need as much storage space as it would using IMAP.

However, because the mail is removed from the server, if the user's computer sustains hard disk damage and lose mail files, there's no way to recover these files without using data backups.

Another advantage of POP is that POP connections are transitory. After the mail is transferred, the connection is dropped and the load on the network and the mail server is removed.

POP isn't the best choice for users who access mail from more than one computer, such as a home computer, an office computer, and a laptop while on the road. When a user retrieves mail via POP, the mail is downloaded to the user's computer and is usually removed from the server. If the user logs in later from a different computer, the user can't see previously downloaded mail.

Internet Message Access Protocol (IMAP)

IMAP is the solution for people who need to use more than one computer to receive mail. IMAP is a client-server mail protocol that allows users to access their mail from anywhere on the Internet. Users can send and read mail with a number of IMAP-compliant mail clients.

With IMAP, a user's mail is delivered to the server and stored in a remote mailbox on the server. To users, mail appears as if it were on the local computer.

A key difference between IMAP and POP is that with IMAP the mail isn't removed from the server until the user deletes it.

The IMAP user's computer can ask the server for message headers, ask for the bodies of specified messages, or search for messages that meet certain criteria. These messages are downloaded as the user opens them.

IMAP connections are persistent and remain open, maintaining load on the server and possibly the network as well.

User Interaction with Mail Service

Mail is delivered to its final recipient using a mail user agent (MUA). MUAs are usually referred to as mail clients or mail applications. These mail clients often run on the user's local computer.

Each user's mail application must be configured to send messages to the correct outgoing server and receive messages from the incoming server. These configurations can affect your server's processing load and available storage space.

Where Mail Is Stored

Mail is stored in an outgoing queue awaiting transfer to a remote server or in a local mail store accessible by local mail users.

Outgoing Mail Location

By default, outgoing mail messages are stored in the following spool directory on the startup disk:
/var/spool/postfix/

This location is temporary, and the mail is stored until it's successfully transferred to the Internet. These locations can be moved to any accessible volume if you use a symlink to the new location.

Incoming Mail Location

Mail service keeps track of incoming mail messages with a small database (BerkeleyDB 4.2.52), but the database doesn't contain the messages. Mail service stores each message as a separate file in a mail folder for each user. Incoming mail is stored on the startup disk in the following directory:
/var/spool/imap/user/[user name]

Cyrus puts a database index file in the user messages folder. You can change the location of mail folders and database indexes to another folder, disk, or disk partition. You can even specify a shared volume on another server as the location of the mail folder and database, although using a shared volume negatively affects performance.

For remotely mounted file systems, NFS isn't recommended. The incoming mail remains on the server until deleted by an MUA.

Cyrus mail storage can also be split across multiple partitions or stored on an XSan cluster. This can be done to scale mail services or to facilitate data backup. For more information see "Creating Additional Mail Store Locations" on page 60.

Maximum Number of Mail Messages Per Volume

Because Mail service stores each mail message in a separate file, the number of messages that can be stored on a volume is determined by the total number of files that can be stored on the volume.

The total number of files that can be stored on a volume that uses Mac OS Extended format (sometimes referred to as *HFS Plus format*) depends on the following factors:

- The size of the volume
- The sizes of the files
- The minimum size of a file, which by default is one 4 KB block

For example, a 4 GB HFS Plus volume with the default block size of 4 KB has one million available blocks. This volume could hold up to a million 4 KB files, which means it can hold a million mail messages that are 4 KB or less each. If some mail messages were larger than 4 KB, this volume could hold fewer of them. A larger volume with the same default block size could hold proportionately more files.

Using Web Service with Mail

WebMail is a web-based mail user agent (MUA). It allows a web browser such as Apple's Safari to compose, read, and forward mail like any other mail client. Mac OS X Server's WebMail functionality is provided by a software package called SquirrelMail at: www.squirrelmail.org.

WebMail relies on your mail server to provide the mail service. WebMail cannot provide mail service independent of the mail server. WebMail uses the mail service of your Mac OS X Server computer.

WebMail uses standard mail protocols and requires your mail server to support them. These protocols are:

- IMAP, for retrieving incoming mail
- SMTP, for exchanging mail with other mail servers (sending outgoing mail and receiving incoming mail)

WebMail doesn't support retrieving incoming mail via POP. Even if your mail server has POP enabled, WebMail doesn't use it.

To use WebMail:

1. Enable and configure your mail server.

   This book has complete setup instructions to get your mail server running.

2. After the mail server is configured, enable the WebMail software.

   For instructions on setting up WebMail, see *Web Technologies Administration*, available at:
   www.apple.com/server/documentation

Using Network Services with Mail Service

Mail service makes use of network services to ensure delivery of mail. Before sending mail, your mail service will probably have a DNS service to determine the Internet Protocol (IP) address of the destination.

The DNS service is necessary because people typically address their outgoing mail by using a domain name, such as example.com, rather than an IP address, such as 198.162.12.12. To send an outgoing message, Mail service must know the IP address of the destination.

Mail service relies on a DNS service to look up domain names and determine the corresponding IP addresses. The DNS service can be provided by your Internet Service Provider (ISP) or by Mac OS X Server, as explained in *Network Services Administration*.

Additionally, a mail exchange (MX) record can provide redundancy by listing an alternate mail host for a domain. If the primary mail host isn't available, the mail can be sent to the alternate mail host. An MX record can list several mail hosts, each with a priority number. If the lowest priority host is busy, mail can be sent to the host with the next lowest priority, and so on.

Without a properly configured MX record in DNS, mail may not reach your intended server.

Mail service use DNS like this:

1. The sending server reads the mail recipient's domain name (it's what comes after the @ in the To address).
2. The sending server looks up the MX record for that domain name to find the receiving server.
3. If found, the message is sent to the receiving server.
4. If the lookup fails to find an MX record for the domain name, the sending server often assumes that the receiving server has the same name as the domain name. So the sending server does an Address (A) lookup on that domain name and attempts to send the file there.

Configuring DNS for Mail Service

Configuring DNS for Mail service entails enabling MX records with your own DNS server. If you have an ISP that provides you with DNS service, contact the ISP so they can enable your MX records. Follow these steps only if you provide your own DNS service using Mac OS X Server.

To enable MX records:

1. In Server Admin, choose a server, then select DNS.
2. Click the Zones button in the toolbar.
3. Select the zone that the MX record will be added to.

   If there are no zones, create one. If the mail server does not have a machine record (A), add one. See *Network Services Administration* for more information.
4. Click the + button in the Mail Exchangers list.
5. Enter the mail server's hostname.
6. Set a mail server precedence number.

   Mail servers try to deliver mail at lower numbered mail servers first.
7. Click OK Save.

To set up multiple servers for redundancy, add additional MX records with different precedence numbers.

How Mail Service Uses SSL

Secure Sockets Layer (SSL) connections ensure that the data sent between your mail server and your users' mail clients is encrypted. This allows secure and confidential transport of mail messages across a local network.

SSL transport doesn't provide secure authentication, just secure transfer from your mail server to your clients. See *Open Directory Administration* for secure authentication information.

For incoming mail, the mail service supports secure mail connections with mail client software that requests them. If a mail client requests an SSL connection, Mail service can comply if that option is enabled. Mail service still provides non-SSL (unencrypted) connections to clients that don't request SSL. The configuration of each mail client determines whether it connects with SSL or not.

For outgoing mail, Mail service supports secure mail connections between SMTP servers. If an SMTP server requests an SSL connection, Mail service can comply if that option is enabled. Mail service can still allow non-SSL (unencrypted) connections to mail servers that don't request SSL.

Enabling Secure Mail Transport with SSL

Mail service requires some configuration to provide SSL connections automatically. The basic steps are as follows:

Step 1: Obtain a security certificate

This can be done in the following ways:

- Get a certificate from a Certificate Authority.
  - Generate a Certificate Signing Request (CSR) and create a keychain.
- Use the CSR to obtain a certificate from an issuing Certificate Authority.Create a self-signed certificate in Server Admin's Certificate Manager.
- Locate an existing certificate from a previous installation of Mac OS X Server v10.3 or later.

If you have already generated a security certificate in a previous version of Mac OS X Server, you can import it for use.

Step 2: Import the certificate into Server Admin's Certificate Manager

You can use Certificate Manager to drag and drop certificate information or you can provide Certificate Manager with the path to an existing installed certificate.

Step 3: Configure the service to use the certificate

For instructions for allowing or requiring SSL transport, see the following sections:

- "Configuring SSL Transport for POP Connections" on page 27
- "Configuring SSL Transport for IMAP Connections" on page 28
- "Configuring SSL Transport for SMTP Connections" on page 31

Before You Begin

Before setting up Mail service for the first time:

- Decide whether to use POP, IMAP, or both for accessing mail.
- If your server will provide mail service over the Internet, obtain a registered domain name.
- Determine whether your ISP will create your MX records or whether you'll create them in your own DNS service.
- Identify the people who will use Mail service but don't have user accounts in a directory domain accessible to Mail service. Then create user accounts for these mail users.
- Determine mail storage requirements and make sure you have enough disk space for your anticipated mail volume.
- Determine your authentication and transport security needs.

How User Account Settings Affect Mail Service

In addition to setting up Mail service as described in this chapter, you can also configure some mail settings individually for anyone who has a user account on your server. Each user account has settings that do the following:

- Enable or disable mail service for the user account, or forward incoming mail for the account to another mail address.
- Specify the server that provides mail service for the user account.
- Set a quota on the amount of disk space for storing the user account's mail on the server.
- Specify the protocol for the user account's incoming mail: POP, IMAP, or both.

Moving Mail Messages from Apple Mail Server to Mac OS X Server v10.5

If you have upgraded your server from a version prior to Mac OS X Server v10.3 and you have an existing Apple Mail Server database, you must migrate your mail database to Mac OS X Server v10.5 Mail service. If you are upgrading from Mac OS X Server v10.3 or v10.4, no migration is necessary.

For more instructions and tool descriptions, see "Converting the Mail Store and Database from an Earlier Version" on page 59.

Overview of Mail Service Tools

The following applications help you set up and manage Mail service:

- *Server Admin:* Use to start, stop, configure, maintain, and monitor Mail service when you install Mac OS X Server.
- *Workgroup Manager:* Use to create user accounts for mail users and configure each user's mail options.
- *Terminal:* Use for tasks that involve UNIX command-line tools, such as backing up and restoring the mail database.

Setup Overview

You can have Mail service set up and start automatically as part of the Mac OS X Server installation process. An option for setting up Mail service appears in the Setup Assistant application, which runs at the conclusion of the installation process. If you select this option, mail service is set up as follows:

- SMTP, POP, and IMAP are active and use standard ports.
- Standard authentication methods are used (not Kerberos), with POP and IMAP set for clear-text passwords (APOP and CRAM MD-5 turned off) and SMTP authentication turned off.
- Mail is delivered only locally (no mail is sent to the Internet).

- Mail relay is restricted.

You can also use the configuration assistant to set up Mail service. This interactive assistant help you select appropriate options and settings.

To start the mail configuration assistant:

1. In Server Admin, select a computer in the Servers list, then select Mail.

   If Mail is not listed beneath the server you selected, Mail service must be started. Click the + button at the bottom of the Servers lists, then select Add Service from the pop-up list.
2. Click the Configure Mail Service button to start the assistant.
3. Follow the onscreen instructions.

Configuring Mail Using Server Admin

To change the mail service manually, these are the major tasks you perform to set up mail service:

Step 1: Make a plan

See "Before You Begin" on page 20 for a list of items to think about before you start full-scale Mail service.

Step 2: Set up MX records

If you want users to be able to send and receive mail over the Internet, make sure DNS service is set up with the appropriate MX records for Mail service:

- If you have an ISP that provides DNS service to your network, contact the ISP and have the ISP set up MX records for you. Your ISP needs to know your mail server's DNS name (such as mail.example.com) and your server's IP address.
- If you use Mac OS X Server to provide DNS service, create MX records as described in "Configuring DNS for Mail Service" on page 19.
- If you do not set up an MX record for your mail server, your server may still be able to exchange mail with other mail servers. Some mail servers will find your mail server by looking in DNS for your server's A record. (You probably have an A record if you have a web server set up.)

Note: Your mail users can send mail to each other even if you do not set up MX records. Local mail service doesn't require MX records.

Step 3: Configure incoming mail service

Mail service has many settings that determine how it handles incoming mail. For instructions, see "Configuring Incoming Mail Service" on page 24.

Step 4: Configure outgoing mail service

Mail service has many settings that determine how it handles outgoing mail. For instructions, see "Configuring Outgoing Mail Service" on page 29.

Step 5: Secure your server

If your server exchanges mail over the Internet, make sure you're not operating an open relay. An open relay is a security risk and enables junk mail senders to use your computer resources for sending unsolicited commercial mail. For instructions see "Limiting Junk Mail and Viruses" on page 43, and "Restricting SMTP Relay" on page 44.

Step 6: Configure additional settings for mail service

Additional settings that you can change affect how mail service stores mail, interacts with DNS service, limits junk mail, and handles undeliverable mail. See the following sections for instructions:

- "Working with the Mail Store and Database" on page 57
- "Limiting Junk Mail and Viruses" on page 43
- "When Mail Is Undeliverable" on page 67

Step 7: Set up accounts for mail users

Each person who wants mail service must have a user account in a directory domain accessible by your mail service. The short name of the user account is the mail account name and is used to form the user's mail address.

In addition, each user account has settings that determine how your mail service handles mail for the user account. You can configure a user's mail settings when you create the user's account, and you can change an existing user's mail settings at any time. For instructions, see "Supporting Mail Users" on page 34, and "Configuring Mail Client Software" on page 34.

Step 8: Create a postmaster alias (optional, but recommended)

You need to create an administrative alias named postmaster. Mail service or the mail administrators send reports to the postmaster account. An alias allows mail sent to postmaster@yourdomain.com to be forwarded to an account of your choice.

Set up forwarding of the postmaster's mail to a mail account that you check regularly. Other common postmaster accounts are named abuse (used to report abuses of your mail service) and spam (used to report unsolicited commercial mail abuses by users).

See "Creating Additional Mail Addresses for a User" on page 35 to learn about creating an alias to an existing mail user.

Step 9: Start Mail service

Before starting mail service, make sure the server computer shows the correct day, time, time zone, and daylight-saving settings in the Date & Time pane of System Preferences. Mail service uses this information to timestamp each message. An incorrect timestamp can cause other mail servers to handle a message incorrectly.

Also, make sure you've enabled one or more mail service protocols (SMTP, POP, or IMAP) in the Settings pane.

After you verify this information, you can start Mail service. If you selected the Server Assistant option to have Mail service start automatically, stop Mail service now, then start it again for your changes to take effect. For detailed instructions, see "Starting and Stopping Mail Service" on page 55.

Step 10: Set up each user's mail client software
After you set up Mail service on your server, mail users must configure their mail client software for Mail service. For details, see "Supporting Mail Users" on page 34.

Configuring Incoming Mail Service

When configuring incoming mail service you configure mail to be retrieved by users and mail client applications. It involves these basic steps:

- Choose and enable the type of access (POP, IMAP, or both).
- Choose a method for authentication of the mail client.
- Choose a policy for secure transport of mail data over SSL.

The following section explains how to accomplish these steps.

Enabling POP Access

POP is used for receiving mail. The POP mail service stores incoming POP mail until users have their computers connect to Mail service and download their waiting mail. After a user's computer downloads POP mail, the mail is stored only on the user's computer.

An advantage of using POP is that your server doesn't need to store mail that users have downloaded.

POP isn't the best choice for users who access mail from more than one computer, such as a home computer, an office computer, and a laptop while on the road because after messages are accessed by one computer, they are deleted from the server.

To enable POP access:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click Enable POP.
5. Click Save.
6. Continue and configure security for POP authentication and transport.

See the following to continue configuration:

- "Enabling Secure POP Authentication" on page 26
- "Enabling Less Secure Authentication for POP" on page 26

- "Configuring SSL Transport for POP Connections" on page 27

Enabling IMAP Access

IMAP is a client-server mail protocol that allows users to access their mail from the Internet. With IMAP, mail is delivered to the server and stored in a remote mailbox on the server. To users, mail appears as if it were on the local computer.

A key difference between IMAP and POP is that with IMAP the mail isn't removed from the server until the user deletes it. IMAP connections are persistent and remain open, maintaining load on the server and possibly the network as well.

To enable IMAP access:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click Enable IMAP.
5. Enter the number of concurrent connections you want to allow, then click Save.

   The maximum is 300.
6. Click Save.
7. Continue and configure security for IMAP authentication and transport.

   See the following to continue configuration:
   - "Enabling Secure IMAP Authentication" on page 27
   - "Enabling Less Secure IMAP Authentication" on page 28
   - "Configuring SSL Transport for IMAP Connections" on page 28

Choosing No Incoming Mail Retrieval

You can choose to enable SMTP mail service, but not supply POP or IMAP service for incoming mail retrieval. If neither POP nor IMAP is enabled, incoming mail from other mail servers is still delivered to users but they can't access their mail with their mail client applications.

Mail that has been accepted for local delivery is queued until POP or IMAP services are enabled, delivery to /var/mail/ is enabled, or the message expires and a Non Delivery Receipt (NDR) is sent to the sender (after 72 hours by default).

If delivery to /var/mail/ is enabled, users can still access mail using UNIX mail tools such as PINE or ELM. Messages delivered to /var/mail/ are not available for delivery to users with Cyrus, if POP or IMAP are enabled again.

If POP and IMAP are disabled, you can change where incoming mail is stored from its default location at /var/spool/imap/user/*user name* to /var/mail/*user name*.

To change the local delivery directory:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click the "Deliver to /var/mail/" checkbox.
5. Click Save.

Enabling Secure POP Authentication

Your POP mail service can protect user passwords by allowing Authenticated POP (APOP) or Kerberos. When a user connects with APOP or Kerberos, the user's mail client software encrypts the user's password before sending it to your POP service. Before configuring Mail service to require secure authentication, make sure that users' mail applications and user accounts support the method of authentication you choose.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. See *Open Directory Administration* for more information.

If you want to *require* either of these authentication methods, enable only one method.

To set the POP authentication method:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click the APOP or Kerberos checkbox in the POP3 list.
6. Click Save.

Enabling Less Secure Authentication for POP

You can allow basic password (clear text) authentication. This is less secure than APOP or Kerberos because the password is transmitted as unencrypted, clear text.

If you want to *require* clear text authentication, enable Clear as the only authentication method.

To enable clear text POP authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.

5 Click the Clear checkbox.

6 Click Save.

Configuring SSL Transport for POP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for POP (and IMAP) connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for POP also sets it for IMAP.

To set SSL transport for POP connections:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Advanced tab.

4 Select Security.

5 Select Require or Use to enable (Don't Use to disable) in the IMAP and POP SSL pop-up menus.

6 Select the certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.

7 Click Save.

Enabling Secure IMAP Authentication

Your IMAP mail service can protect user passwords by requiring that connections use a secure method of authentication. You can choose CRAM-MD5, or Kerberos v5 authentication. When a user connects with secure authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Make sure that your users' mail applications and user accounts support the method of authentication you choose.

If you configure Mail service to require CRAM-MD5, you must set mail accounts to use a Mac OS X Server Password Server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see *Open Directory Administration* for more information.

If you want to *require* any of these authentication methods, enable only one method.

To set secure IMAP authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Select CRAM MD-5 or Kerberos (as desired) in the IMAP section.
6. Click Save.

Enabling Less Secure IMAP Authentication

Your IMAP mail service can supply users passwords by less secure means. These authentication methods are less secure because they don't securely encrypt users passwords as they cross the network.

If you want to *require* any of these authentication methods, enable only one method.

To allow login, plain, or clear IMAP authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click the LOGIN, PLAIN, or Clear checkbox in the IMAP list.
6. Click Save.

Configuring SSL Transport for IMAP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for IMAP also sets it for POP.

To configure SSL transport for IMAP connections:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click Require or Use to enable (Don't Use to disable) from the pop-up menus in the IMAP and POP SSL section.
6. Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
7. Click Save.

Configuring Outgoing Mail Service

Mail service includes an SMTP service for sending mail. Subject to restrictions that you control, the SMTP service also transfers mail to and from Mail services on other servers.

If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service. Other mail services deliver messages for your mail users to your SMTP service, which then transfers the messages to your POP service and IMAP service.

Enabling SMTP Access

SMTP is used for transferring mail between mail service and sending mail from user's mail clients. The SMTP mail service stores outgoing mail in a queue until it has found the mail exchange server at the mail's destination. Then it transfers the mail to the destination server for handling and eventual delivery.

SMTP service is required for outgoing mail service and for accepting delivery of mail from mail servers outside your organization.

To enable SMTP access:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click Enable SMTP.
5. Select "Allow incoming mail," if desired.
6. If you allow incoming mail, enter the domain name to accept mail for, and the mail server's host name.
7. Click Save.

Understanding SMTP Authentication

If you don't choose any method of SMTP authentication or authorized specific SMTP servers to relay for, the SMTP server will allow anonymous SMTP mail relay, and is considered an open relay. Open relays are bad because junk mail senders can exploit the relay to hide their identities and send illegal junk mail without penalty.

There is a difference between *relaying mail* and *accepting delivery of mail*. Relaying mail means passing mail from one (possibly external) mail server or a local user's mail client to another (third) mail server. Accepting delivery means receiving mail from a (possibly external) mail server to be delivered to the server's mail users. Mail addressed to local recipients is still accepted and delivered. Enabling authentication for SMTP *requires* authentication from any of the selected authentication methods prior to *relaying mail*.

SMTP Authentication is used in with restricted SMTP mail transfer to limit junk mail propagation. For more information about these settings, see "Limiting Junk Mail and Viruses" on page 43.

Enabling Secure SMTP Authentication

Your server can guard against being an open relay by allowing SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) You can configure the mail service to require secure authentication using CRAM-MD5 or Kerberos. You can also allow the less secure plain and login authentication methods, which don't encrypt passwords, if some users have mail client software that doesn't support the secure methods.

If you configure your mail service to require CRAM-MD5, mail users' accounts must be set to use a password server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see *Open Directory Administration*.

Enabling SMTP Authentication will:

- Make your users authenticate with their mail client before accepting mail to send.
- Frustrate mail server abusers trying to send mail without your consent through your system.

If you want to *require* any of these authentication methods, enable only one method.

To allow secure SMTP authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click the CRAM MD-5, or Kerberos checkbox in the SMTP section.
6. Click Save.

Enabling Less Secure SMTP Authentication

Your server can guard against being an open relay by requiring SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) Requiring authentication ensures that only known users—people with user accounts on your server—can send mail from your mail service. You can choose to require, allow, or disallow less secure authentication methods (plain text or login) for SMTP mail service.

Plain authentication sends mail passwords as plain text over the network. Login authentication sends a minimally secure crypt hash of the password over the network.

If you want to *require* any of these authentication methods, enable only one method.

To allow less secure authentication:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click either Plain or Login checkbox in the SMTP section.
6. Click Save.

Configuring SSL Transport for SMTP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

To configure SSL transport for SMTP connections:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Security.
5. Click Require or Use to enable (or Don't Use to disable) in the SMTP SSL section.
6. Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
7. Click Save.

Relaying SMTP Mail Through Another Server

Rather than delivering outgoing mail to its various destinations, your SMTP mail service can relay outgoing mail to another server.

Normally, when an SMTP server receives a message addressed to a remote recipient, it attempts to send that message to that server or the server specified in the MX record, if it exists. Depending on your network setup, this method of mail transport might not be desired or even possible. You might then need to relay outbound messages through a specific server.

You might need to use this method to deliver outgoing mail through the firewall set up by your organization. In this case, your organization will designate a server for relaying mail through the firewall.

This method can be useful if your server has slow or intermittent connections to the Internet.

Do not attempt to relay mail through a mail server outside your organization's control without the relay administrator's permission. Trying to do so will label you as a mail service abuser.

To relay SMTP mail through another server:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Click the General tab.
4. Click "Relay outgoing mail through host" and enter the DNS name or IP address of the server that provides SMTP relay.
5. Click Save.

Limiting Incoming Message Size

You can set a maximum size for incoming messages. The default is 10 MB. You might not want to allow large attachments that add to the message size.

To set a maximum incoming message size:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Click the Quotas tab.
4. Click the "Refuse messages larger than" checkbox and enter the number of megabytes you want to set as the limit.
5. Click Save.

Using ACLs for Mail Service Access

Access Control Lists (ACLs) are a method of designating service access to specific users or groups on an individual basis. For example, you can use an ACL to allow only one user access to a file server or shell login, without allowing any user on the server to access it.

Mail services are different from many other services that traditionally use ACLs for determining service access. Mail service is already specified on a per-user basis. Either you have a mail account on a server or you don't. Being a user on a server doesn't automatically confer access to mail storage and retrieval.

Some administrators may find it easier to designate mail access using ACLs if they are doing all their other configuration using ACLs. They also may have mixed network environments that necessitate using ACLs to assign mail access.

Mac OS X Server allows you to enable mail access for users using the Access tab in a server's Server Admin listing. If you enabled user access via Server Admin and traditional mail access using Workgroup Manager, the settings interact in the following manner:

Access via ACL	Access via Workgroup Manager	Result
On	On	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
On	Off	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
Off	On	User has mail access granted according to his or her user record settings in Workgroup Manager. This is the default.
Off	Off	User has no mail access.

To enable a user's mail access using ACLs:

1. In Server Admin, select the server that has Mail service running and then click Settings.
2. Select Access, then click Services.
3. Select Mail from the Services list.
4. Deselect "Use same access for all services."
5. Select "Allow only users and group below."
6. Click the Add (+) button to reveal a Users and Groups list.
7. Drag the user to the access list.
8. Click Save.

Supporting Mail Users

This section discusses mail settings in your server's user accounts, user mail storage quotas, and mail service settings in mail client software.

Configuring Mail Settings for User Accounts

To make Mail service available to users, you must configure mail settings in your user accounts. For each user, you need to:

- Enable mail usage.
- Enter the DNS name or IP address of your mail server.
- Select the protocols for retrieving incoming mail (POP, IMAP, or both).
- Set a quota on disk space available for storing a user's mail.
- Configure any alternate mail storage location.

You configure these settings with the Workgroup Manager application. For detailed instructions, see *User Management*.

Configuring Mail Client Software

Users must configure their mail client software to connect to Mail service. The following table details the information most mail clients need and the source of the information in Mac OS X Server.

Mail client software	Mac OS X Server	Example
User name	Full name of the user	Steve Macintosh
Account name or Account ID	Short name of user account	steve
Password	Password of user account	
Host name Mail server Mail host	Mail server's full DNS name or IP address, as used when you log in to the server in Server Admin	mail.example.com 192.168.50.1
Mail address	User's short name, followed by the @ symbol, followed by one of the following: • Server's Internet domain (if the mail server has an MX record in DNS) • Mail server's full DNS name • Server's IP address in brackets	steve@example.com steve@mail.example.com steve@[192.168.50.1]
SMTP host SMTP server	Same as host name	mail.example.com 192.168.50.1
POP host POP server	Same as host name	mail.example.com 192.168.50.1
IMAP host IMAP server	Same as host name	mail.example.com 192.168.50.1

Mail client software	Mac OS X Server	Example
SMTP user	Short name of user account	steve
SMTP password	Password of user account	

Creating an Administration Account

You may need to create a mail administrator account to maintain and watch mail folders, remove defunct user accounts, and archive mail. This administrator account doesn't need to be a server administrator. Also, this administrator account shouldn't receive mail. It isn't a normal mail account.

To create a mail administrator account:

1. Designate a user to be mail administrator.
2. If you haven't created a user account for the mail administrator, see *User Management*.
3. Open /etc/imapd.conf in a text editor.

   If you aren't comfortable using a Terminal-based text editor like emacs or vi, you can use TextEdit.
4. Find the line that reads "admins:"
5. Edit the line to add the short name of the administrator account after the colon.
6. Save your changes.

For more information see the man page for imapd.conf.

Creating Additional Mail Addresses for a User

Mail service allows each user to have more than one mail address, called an alias. Every user has one mail address that's formed from the short name of the user account. In addition, you can define more names for any user account by creating an alias file. Each additional name is an alternate mail address for the user at the same domain. These additional mail addresses aren't additional accounts and don't require separate quotas or passwords.

Most often, alias files are used to map postmaster users to a real account and give a "firstname.lastname@example.com" mail address to a user with a short login account name.

There are two methods for creating mail aliases: Mac OS X Server–style, and Postfix-style. Each has its advantages and disadvantages.

- Mac OS X Server–style aliases are easy to make and are listed with a user's login name. You can easily see what alias refers to which user. The disadvantage of this is that mail service's Sieve functionality doesn't understand Mac OS X Server–style aliases and can't filter mail based on the Mac OS X Server–style alias.

- Postfix-style aliases require command-line administration, and are less obvious to audit. However, the major benefit to using Postfix-style aliases is their compatibility with Sieve scripting. Only aliases generated Postfix-style can be acted upon by Sieve scripts.

If you are using this feature with virtual mail hosting and are using Mac OS X v10.4.3 or later, you must enter a fully-qualified mail address (i.e. *username@domain_name*) in the location indicated in Workgroup Manager.

To create a Mac OS X Server–style alias:

1. In Workgroup Manager, open the user account you want to work with, if it isn't already open.

   To open the account, click the Accounts button, click the globe icon below the toolbar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
2. Click the Basic tab.
3. Double-click under the last entry in the Short Names field.
4. Enter the alias.

   For example, if your domain is example.com and you want to give user name bob an alias of robert.fakeuser you should enter:

   ```
   robert.fakeuser
   ```

   If virtual hosting is enabled, enter the fully qualified mail address:

   ```
   robert.fakeuser@example.com
   ```
5. Click Save.

   As a result, mail to robert.fakeuser@example.com is sent to user bob, giving Bob two effective mail addresses, bob@example.com and robert.fakeuser@example.com.

To create a Postfix-style alias:

1. Create the file /etc/postfix/aliases, if none exists.
2. For each alias, make a line in the file with the following format:

   alias:localaddress1,localaddress2,...

   For example, for your domain example.com, if you want to give user name bob"an alias of robert.fakeuser you enter:

   ```
   robert.fakeuser: bob
   ```

   This takes mail sent to your mail server for robert.fakeuser@example.com and sends it to the real mail account, bob@example.com.
3. Save your file changes.

4 In the Terminal application, enter the following command:

```
postalias /etc/postfix/aliases
```

The text file is processed into a database for faster access.

5 At the prompt, enter the following command:

```
newaliases
```

The alias database will reload.

As a result, mail to robert.fakeuser@example.com will be sent to user bob, giving Bob two effective mail addresses, bob@example.com and robert.fakeuser@example.com.

For further information about creating and maintaining mail aliases, refer to /etc/postfix/aliases.

Setting Up Forwarding Mail Addresses for a User

You can use forwarding to provide a mail redirection service for users. Any mail sent to a user's mail account is forwarded to the specified account.

There is an additional method of mail forwarding using Sieve scripting. To learn more about that method, see "Sieve Scripting Support" on page 51.

To forward a user's mail:

1 In Workgroup Manager, open the user account you want to work with, if it isn't already open.

To open the account, click the Accounts button, click the globe icon below the toolbar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

2 Click the Mail tab.

3 Select Forward.

4 Enter the forwarding mail address in the Forward To field.

You can enter multiple addresses but they must be separated by a comma.

Virtual hosting is a method you can use to host more than one domain name on the same computer and IP address, with overlapping mail user names.

For instance, a mail server can receive mail transfer requests for two domains, mail.example1.com and mail.example.com, both of which resolve to the same IP address. For mail.example1.com, the server would deliver mail to "bob@example1.com" to a user mailbox for "bob," while it would also deliver mail to "bob@example2.com" to a *different* user mailbox. Virtual hosts are essentially the converse of local host aliases.

Enabling Virtual Hosting

Before you can enable virtual hosting, you must add a list of locally hosted virtual domains to your mail server. If you enable virtual domains, mail aliases (as described in "Creating Additional Mail Addresses for a User" on page 35) as well as mail addresses associated with the virtual name (as described in "Associating Users to the Virtual Host" on page 39) must be fully qualified. This means that additional mail user names entered into the Short Names field of a user's Workgroup Manager record must contain the user name as well as the "@domainname" portion.

If you enable hosted virtual domains, you must include (in Workgroup Manager's Short Name field for a user) the user's full mail address for all mail hosts you expect the user to receive mail, for all aliases and virtual host addresses.

To enable virtual hosting:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Hosting.
5. Add at least one virtual host.

   See "Adding or Removing Virtual Hosts" for more information.
6. Select Enable Virtual Hosting.

   You can now add or remove virtual hosts using the Add (+) or Remove (–) button.
7. Click Save.

Adding or Removing Virtual Hosts

Before you can enable virtual hosting, you must add a list of locally hosted virtual domains to your mail server. Virtual hosting must be enabled to add or remove virtual hosts. If virtual hosting is not enabled, see "Enabling Virtual Hosting" on page 38.

If you enable virtual host domains, all mail aliases, addresses for local host aliases, and mail addresses associated with the virtual name must be fully qualified. This means that additional mail user names entered into the Short Names field of a user's Workgroup Manager must contain the user name as well as the @domainname portion.

If you enable virtual domains, you must include the full mail address for both user aliases *and* virtual users.

To add or remove virtual hosts:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Advanced tab.
4. Select Hosting.

5 Click the Add (+) button next to the Locally Hosted Virtual Domain box and enter the domain name of a virtual host you want your server to be responsible for.

To change a virtual domain, select it, and click the Edit (/) button.

To remove an item from the list, select it and click the Remove (–) button.

6 Click Save.

Note: Set up MX records for each virtual domain. If a domain name in this list doesn't have an MX record, only your mail service recognizes it. External mail sent to this domain name is returned.

Associating Users to the Virtual Host

Associating users to a virtual host requires creating an alias in their user records which contain the entire mail address (such as bob@example.com, where example.com isn't the domain name of the mail server, but a virtual host).

There are two methods for creating aliases for virtual host users: Mac OS X Server–style, and Postfix-style. Each has its advantages and disadvantages:

- Mac OS X Server–style aliases are easy to make, and are listed with a user's login name. You can easily see what alias refers to which user. The downside is that mail service's Sieve functionality doesn't understand Mac OS X Server–style aliases and will not filter mail based on the Mac OS X Server–style alias.
- Postfix-style aliases require command-line administration, and are less obvious to audit. However, Postfix-style aliases are compatible with Sieve scripting. Only aliases generated by the Postfix-style method can be acted upon by Sieve scripts.

To associate a user to a virtual host using Mac OS X Server–style aliases:

1 Add a Virtual Host Name using the directions in the section "Adding or Removing Virtual Hosts" on page 38.

2 In Workgroup Manager, open the user account you want to work with, if it isn't already open.

To open the account, click the Accounts button, then click the globe icon below the toolbar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

3 Click Basic, then double-click under the last entry in the Short Names field.

4 Enter the user name and the fully qualified mail address at the virtual host (*name@virtualhostdomain*).

For example, if your domain is example.com and the virtual host domain is server.com, and you want mail addressed to postmaster@server.com to be delivered to user bob, open bob's user record in Workgroup Manager, and enter:

```
postmaster@server.com
```

Note: You must use the entire mail address for this to work for a virtual mail host. If you only enter the new user name without the remainder of the address, you may have made an alias for the user on the default domain, rather than the virtually hosted domain.

5 Click Save.

This causes mail sent to your mail server for postmaster@server.com to be actually sent to the real mail account for user bob. Meanwhile, mail to postmaster@example.com will go to another designated mail account.

To associate a user to a virtual host using Postfix-style aliases:

1 Add a Virtual Host Name using the directions in "Adding or Removing Virtual Hosts" on page 38.

2 Log in to Terminal as the root user.

3 Save the original virtual user file to be used as a future template by entering the following command:

```
cp /etc/postfix/virtual /etc/postfix/virtual.original
```

4 Using a text editor as the root user, open and edit the file /etc/postfix/virtual by adding the following line at the beginning of each section (one section for each virtual host):

```
virtual_host_domain virtual
```

Fill in the virtual host domain name as appropriate. For example, if your virtual host domain is server.com substitute that domain name for virtual_host_domain above. This distinguishes the section as belonging to a specific virtual domain.

This is necessary if you only have one virtual domain, or if you have Mailing Lists enabled for your virtual domains.

5 For each virtual user, add a line in the file with the following format:

name@virtual_host_domain local_user_name

For example, if your domain is example.com and you are running a virtual host for "server.com," and if you want to have the user bob get mail sent to "postmaster@server.com," you should enter:

```
postmaster@server.com bob
```

This causes mail sent to your mail server for postmaster@server.com to be sent to user "bob." Mail sent to postmaster@example.com will be sent to some other designated recipient.

You can make a catch-all address to get all mail not sent to an existing user by using the following format:

@virtual_host_domain local_user_name

This is not recommended because it can increase the amount of junk mail you receive.

6 Save your file changes.

7 Using a text editor as the root user, add a configuration line to /etc/postfix/main.cf so Postfix knows where to look for the virtual user file, if the line doesn't already exist:

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

8 At the prompt, enter the following command:

```
postmap /etc/postfix/virtual
```

The virtual user file is processed for access by Postfix.

9 At the prompt, reload the mail server settings by entering the following command:

```
postfix reload
```

This causes mail sent to your mail server for postmaster@server.com to be sent to the real mail account for user bob. Meanwhile, mail to postmaster@example.com will go to another designated mail account.

Managing Mail Quotas

Mail quotas define how much disk space a user's mail can use on the mail server. Quotas are set on a per-user basis in the user's record in Workgroup Manager. Although you don't set an mail user's quota in Server Admin, you do manage quota enforcement and your server's response to quota violation.

Mail quotas are especially important if the mail server hosts many IMAP accounts. IMAP doesn't require mail to be removed from the server when read, so IMAP users who get large attachments can fill their quotas very quickly.

Enabling Mail Quotas for Users

You can enable limits to mail storage on server. This is especially important if you use IMAP for incoming messages because mail messages aren't necessarily deleted when downloaded to the user.

You use Workgroup Manager to enable a user's mail quota.

To enable a user's mail quota:

1 In Workgroup Manager, open the user account you want to work with, if it isn't already open.

To open the account, click the Accounts button, click the globe icon below the tool bar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

2 Click the Mail tab.

If the user doesn't have mail enabled, enable it now.

3 Enter the number of MB for the user's mail storage in the Mail Quota box.

4 Click Save.

Configuring Quota Warnings

When a user's mailbox approaches its storage quota, you can warn users of an impending quota violation. You choose whether to warn the mail user, how often to warn him or her, and at what point to send the warning.

To configure quota warnings:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Quotas tab.
4. Click Enable Quota Warnings.
5. Enter the maximum percentage of storage usage before a warning is sent.
6. Enter the frequency of the warning notice, in number of days.
7. If you want to customize the quota warning notification, click Edit Quota Warning Message and then customize the message.
8. Click Save.

Configure Quota Violation Responses

When a mail user has more mail in storage than is allowed for his or her quota, the mail server recognizes a quota violation. There are typically two responses to quota violation: a violation notice, and suspension of mail service.

To configure quota violation responses:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Quotas tab.
4. Click Enable Quota Warnings.
5. If you want to customize the quota violation notification, click Edit Quota Warning Message, then customize the message.
6. If you want to suspend mail service for users who exceed their quotas, select "Disable a user's incoming mail when they exceed 100% of quota."
7. If you want to customize the over quota message, click Edit Over Quota Error Message and then customize the message.
8. Click Save.

Limiting Junk Mail and Viruses

You can configure Mail service to decrease the volume of unsolicited commercial mail, also known as junk mail (or spam), and mail containing viruses. You can take steps to block junk mail or viruses that are sent to your mail users. Additionally, you can secure your server against use by mail service abusers, who try to use your resources to send junk mail to others.

You can also take steps to prevent senders of junk mail from using your server as a relay point. A relay point or open relay is a server that unselectively receives and forwards mail addressed to other servers. An open relay sends mail from any domain to any domain.

Junk mail senders exploit open relay servers to avoid having their own SMTP servers blacklisted as sources of junk mail. You don't want your server blacklisted as an open relay because other servers may reject mail from your users.

There are two main methods of preventing viruses and junk mail passing through or into your mail system. Using both of the methods in concert will help ensure your mail system integrity. The two points of control are:

- "Connection Control" (below)
- "Mail Screening" on page 47

Connection Control

This method of prevention controls which servers can connect to your mail system and what those servers must do to send mail through your mail system. Your mail service can do any of the following to exercise connection control:

- Require SMTP authentication
- Restrict SMTP relay, allowing relay only by approved servers
- Reject all SMTP connections from disapproved servers
- Reject mail from blacklisted servers
- Filter SMTP connections

These methods are explained on the following pages.

Requiring SMTP Authentication

If your mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server.

Although SMTP authentication applies primarily to mail relay, your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they can't send mail to remote servers. Mail sent from external mail servers and addressed to local recipients is still accepted and delivered.

To require SMTP authentication, see "Enabling Secure SMTP Authentication" on page 30 and "Enabling Less Secure SMTP Authentication" on page 31.

Restricting SMTP Relay

Your mail service can restrict SMTP relay by allowing only approved hosts to relay mail. You create the list of approved servers.

Approved hosts can relay through your mail service without authenticating. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All hosts, approved or not, can deliver mail to your local mail users without authenticating.

Your mail service can log connection attempts made by hosts not on your approved list.

To restrict SMTP relay:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Accept SMTP relays only from these" checkbox.
5. Edit the list of hosts:
   - Click the Add (+) button to add a host to the list.
   - Click the Remove (–) button to delete the currently selected host from the list.
   - Click the Edit (/) button to change the currently selected host from the list.

   When adding to the list, you can use a variety of notations.
   - Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21.
   - Enter a host name, such as mail.example.com.
   - Enter an Internet domain name, such as example.com.

SMTP Authentication and Restricted SMTP Relay Combinations

The following table describes the results of using SMTP authentication and restricted SMTP relay in various combinations.

SMTP requires authentication	Restricted SMTP relay	Result
On	Off	All mail servers must authenticate before your mail service will accept mail for relay. Your local mail users must also authenticate to send mail out.
On	On	Approved mail servers can relay without authentication. Servers you haven't approved can relay after authenticating with your mail service.
Off	On	Your mail service can't be used for open relay. Approved mail servers can relay (without authenticating). Servers that you haven't approved can't relay unless they authenticate, but they can deliver to your local mail users. Your local mail users don't need to authenticate to send mail. This is the most common configuration.

Rejecting SMTP Connections from Specific Servers

Your mail service can reject unauthorized SMTP connections from hosts on a disapproved-hosts list that you create. All mail traffic from hosts on this list is denied and the SMTP connections are closed after posting a 554 SMTP connection refused error.

To reject unauthorized SMTP connections from specific servers:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Refuse all messages from these" checkbox.
5. Edit the list of servers:
   - Click the Add (+) button to add a host to the list.
   - Click the Remove (–) button to delete the selected host from the list.
   - Click the Edit (/) button to change the selected host from the list.

When adding to the list, you can use the following notations:

Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21. Enter a host name, such as mail.example.com. Enter an Internet domain name, such as example.com.

Rejecting Mail from Blacklisted Senders

Your mail service can reject mail from SMTP servers that are blacklisted as open relays by a Real-time Blacklist (RBL) Server. Your mail service uses an RBL server that you specify. RBLs are sometimes called *black-hole servers*.

Blocking unsolicited mail from blacklisted senders may not be completely accurate. Sometimes it prevents valid mail from being received.

To reject mail from blacklisted senders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Relay tab.
4. Click the "Use these junk mail rejection servers" checkbox.
5. Edit the list of servers by adding the DNS name of an RBL server.:
   - Click the Add (+) button to add a server to the list, then enter the domain name of a RBL server, such as rbl.example.com.
   - Click the Remove (–) button to delete the selected server from the list.
   - Click the Edit (/) button to change the selected server.

Filtering SMTP Connections

You can use Firewall service of Mac OS X Server to allow or deny access to your SMTP mail service from specific IP addresses. Filtering disallows communication between an originating host and your mail server. Mail service doesn't receive the incoming connection and no SMTP error is generated or sent back to the client.

To filter SMTP connections:

1. In Server Admin, select Firewall in the Computers & Services pane.
2. Create a firewall IP filter using the instructions in *Network Services Administration,* using the following settings:
   - Access: denied
   - Port number: 25 (or your incoming SMTP port, if you use a nonstandard port)
   - Protocol: TCP
   - Source: the IP address or address range you want to block
   - Destination: your mail server's IP address
3. If desired, log the packets to monitor the SMTP abuse.
4. Add more filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information about the firewall service, see *Network Services Administration*.

Mail Screening

After a mail delivery connection is made and the message is accepted for local delivery (relayed mail is not screened), the mail server can screen it before delivery. Mac OS X Server uses SpamAssassin (from spamassassin.apache.org) to analyze the text of a message, and gives it a probability rating for being junk mail.

No junk mail filter is 100% accurate in identifying unwanted mail. For this reason the junk mail filter in Mac OS X Server doesn't delete or remove junk mail from being delivered. Instead it marks the mail as potential junk mail.

The user can then decide if it's really unsolicited commercial mail and deal with it accordingly. Many mail clients use the ratings that SpamAssassin adds as a guide in classifying mail for the user.

Mac OS X Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can deal with it in several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

Enabling Junk Mail Screening (Bayesian Filters)

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure certain screening parameters.

Bayesian mail filtering is the classification of mail messages based on statistics. Each message is analyzed and the word frequency statistics are saved. Mail messages that have more of the same words as those in junk mail receive a higher marking of probability that they are also junk mail. When the message is screened, the server adds a header ("X-Spam-Level") with the junk mail probability score.

For example, let's say you have 400 mail messages where 200 of them are junk mail and 200 are good mail. When a message arrives, its text is compared to the 200 junk mail, and the 200 good messages. The filter assigns the incoming message a probability of being junk or good, depending on what group it most resembles.

Bayesian filtering has shown itself to be a very effective method of finding junk mail, if the filter has enough data to compare. One of the strengths of this method is the more mail you get and classify (a process called training), the more accurate the next round of classification is. Even if junk mail senders alter their mailings, the filter takes that into account the next time around.

To enable junk mail screening:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Mail for Junk Mail.

5 Set the level of permissiveness (Cautious, Moderate, Aggressive).

The permissiveness meter sets how many junk mail flags can be applied to a single message before it is processed as junk mail. If you set it to "Least permissive," any mildly suspicious mail is tagged and processed as junk mail. If you set it to "Most permissive" it takes a high score (in other words, many junk mail characteristics) to mark it as junk.

6 Decide how to deal with junk mail messages.

- *Bounced*: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
- *Deleted*: Deletes the message without delivery. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
- *Delivered*: Delivers the message even though it's probably junk mail. You can optionally add text to the subject line, indicating that the message is probably junk mail, or encapsulate the junk mail as a MIME attachment.
- *Redirected*: Delivers the message to someone other than the intended recipient.

7 Choose how often to update the junk mail database updated, if desired.

8 Click Save.

For an explanation of other options, see "Filtering Mail by Language and Locale" on page 49.

Manually Training the Junk Mail Filter

It's important to teach the filter what is and what isn't junk mail. Initially, the filter won't be very accurate at marking junk mail, but you can train it to do better. Accurate training requires a large sample, so a minimum of 200 messages of each type is advised.

To train the filter:

1 Choose a mailbox of 200 messages made of only junk mail.

2 Use Terminal and the filter's command-line training tool to analyze it and remember it as junk mail using the following command:

```
sa-learn --showdots --spam <junk mail directory>/*
```

3 Choose a mailbox of 200 messages made of only good mail.

4 Use Terminal and the filter's command-line training tool to analyze it and remember it as good mail using the following command:

```
sa-learn --showdots --ham <junk mail directory>/*
```

If the junk mail filter fails to identify a junk mail message, train it again so it can do better next time. Use `sa-learn` again with the `--spam` argument on the mislabeled message. Likewise, if you get a false positive (a good message marked as junk mail), use `sa-learn` again with the `--ham` argument to further train the filter.

Automatically Training the Junk Mail Filter

The junk mail filter must be told what is and isn't junk mail. Mac OS X Server provides a method of automatically training the filter with the help of mail users. The server runs an automated command at 1 am (a cron job) that scans two specially named mail users' in boxes. It runs SpamAssassin's sa-learn tool on the contents of the in boxes and uses the results for its adaptive junk mail filter.

To automatically train the junk mail filter:

1. Enable junk mail filtering.

   See "Enabling Junk Mail Screening (Bayesian Filters)" on page 47 .

2. Create two local accounts: junkmail and notjunkmail.
3. Use Workgroup Manager to enable them to receive mail.

   If you need help with this, see "Configuring Mail Settings for User Accounts" on page 34.

4. Instruct your mail users to redirect junk mail messages which have not previously been tagged as junk mail to junkmail@<yourdomain>.
5. Instruct your mail users to redirect real mail messages that were wrongly tagged as junk mail to notjunkmail@<yourdomain>.

   Each day at 1 am, the junk mail filter will learn what is junk and what was mistaken for junk, but is not.

6. Delete the messages in the junkmail and notjunkmail accounts daily.

Filtering Mail by Language and Locale

You may decide to filter incoming mail based on locales or languages. Mail messages composed in foreign text encodings are often erroneously marked as junk mail. You can configure your mail server to not mark messages from designated originating countries or languages as junk mail.

To allow mail by language and locale:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Junk Mail.
5. Click the Edit (/) button next to Accepted Languages to change the list. Select the language encodings to allow as non-junk mail, and click OK.
6. Click the Edit (/) button next to Accepted Locales to change the list. Select the country codes to allow as non-junk mail, and click OK.
7. Click Save.

Enabling Virus Screening

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

Mac OS X Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can choose to deal with it several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

To enable virus screening:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Filters tab.
4. Select Scan Email for Viruses.
5. Decide how to deal with junk mail messages.

   Bounced: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account (probably the domain's postmaster) and notify the intended recipient.

   Deleted: Deletes the message without delivery. You can optionally send an mail notification to some mail account, probably the postmaster, as well as the intended recipient.

   Quarantined: Delivers the message to a directory for further analysis. You can optionally send an mail notification of the quarantine to some mail account, probably the postmaster.
6. Choose if you want to notify the intended recipient if the message was filtered.
7. Choose how often to update the virus database.

   A minimum of twice a day is suggested. Some administrators choose eight times a day.
8. Click Save.

Advanced Configuration Tools and Options

Mac OS X Server ships with powerful tools to help administer you mail service. These advanced configuration tools use the command line, require a basic familiarity with working within a shell, and require basic scripting concepts.

cyradm

The tool cyradm is included with Mac OS X Server. It is an administration shell for Cyrus, the IMAP mail service package. It communicates with the Cyrus:IMAP::Admin Perl module.

Cyradm can be used to create, delete or rename mailboxes, as well as set ACLs for mailboxes (for mail clients that support them).

Note the following:

- Cyradm is a limited shell: It supports shell-style redirection, but does not understand pipes.
- Cyradm can be used interactively or it can be scripted, but Perl scripting with Cyrus::IMAP::Admin will be more flexible.
- All spaces in file or directory names must be escaped with a "\" as you would in a shell.

For a complete list of commands for cyradm, consult its man page in Terminal by entering: man cyradm

Sieve Scripting Support

Mac OS X Server supports Sieve scripting for mail processing. Sieve is an Internet standard mail filtering language for server-side filtering. Sieve scripts interact with incoming mail before final delivery.

Sieve acts much like the rules in various mail programs to sort or process mail based on user-defined criteria. In fact, some mail clients use Sieve for client-side mail processing. Sieve can provide such functions as vacation notifications, message sorting, and mail forwarding.

Sieve scripts are kept for each user on the mail server at:

/usr/sieve/*first_letter_of_user_name/user_name/*

The directory is owned by the mail service, so users normally don't have access to it, and can't put their scripts there for mail processing. For security purposes, users and administrators upload their scripts to a Sieve process (timsieved) which transports the scripts to the mail process for use.

There are various ways of getting the scripts to timsieved: Perl shell scripts (sieveshell, not included with Mac OS X Server), web mail plugins (avelsieve, not included with Mac OS X Server), and even some mail clients.

Enabling Sieve Support

In order for Sieve to function, you must enable its communications port. By default, Sieve has the vacation extension. All scripts must be placed in the central script repository at /usr/sieve/, and Sieve scripts cannot be used to process mail for mail aliases set up in Workgroup Manager; you must use Postfix-style aliases.

To enable Sieve support:

1. Add the following entry in /etc/services/:

```
sieve 2000/tcp #Sieve mail filtering
```

2. Reload the mail service.

Learning Sieve Scripting

Sieve's complete syntax, commands, and arguments are found in IETF RFC 3028 at www.ietf.org/rfc/rfc3028.txt?number=3028

Other information about Sieve and a sample script archive can be found at www.cyrusoft.com/sieve

Sample Sieve Scripts

The following scripts are examples of common scripts a user might want to use.

Vacation Notification Script

```
#--------
# This is a sample script for vacation rules.
# Read the comments following the pound/hash to find out
# what the script is doing.
#---------
#
# Make sure the vacation extension is used.
require "vacation";
# Define the script as a vacation script
  vacation
# Send the vacation response to any given sender only once every seven days
     no matter how many messages are sent from him.
  :days 7
#For every message sent to these addresses
  :addresses ["bob@example.com", "robert.fakeuser@server.com"]
# Make a message with the following subject
  :subject "Out of Office Reply"
# And make the body of the message the following
"I'm out of the office and will return on December 31. I won't be able to
     replay until 6 months after that. Love, Bob.";
# End of Script
```

Self-Defined Forwarding

```
#--------
# This is a sample script to illustrate how Sieve could be used
# to let users handle their own mail forwarding needs.
```

```
# Read the comments following the pound/hash to find out what the
# script is doing.
#---------
#
# No need to add any extension. 'redirect' is built-in.
# Redirect all my incoming mail to the listed address
redirect "my-other-address@example.com";
# But keep a copy of it on the IMAP server
    keep;
# End of script
```

Basic Sort and Antijunk Mail Filter

```
#--------
# This is a sample script to show discarding and filing.
# Read the comments following the pound/hash to find out
# what the script is doing
#---------
#
# Make sure filing and rejection are enabled
require "fileinto";
#
# If it's from my mom...
if header ["From"] :contains ["Mom"]{
# send it to my home email account
     redirect "home-address@example.com";
  }
#
# If the subject line has a certain keyword...
else if header "Subject" :contains "daffodil" {
# forward it to the postmaster
     forward "postmaster@server.edu";
  }
#
# If the junk mail filter has marked this as junk...
else if header :contains ["X-Spam-Flag"] ["YES"]{
# throw it out
     discard;
  }
#
# If the junk mail filter thinks this is probably junk
else if header :contains ["X-Spam-Level"] ["***"]{
# put it in my junkmail box for me to check
     fileinto "INBOX.JunkMail";
  }
#
# for all other cases...
else {
# put it in my inbox
     fileinto "INBOX";
  }
# End of script
```

Configuring Additional Mail Service Support for 8-Bit MIME

By default, many mail systems that use 8-bit character encoding for text (like Asian language mail systems) converted from 8-bit MIME to 7-bit characters. This has the unfortunate side effect of rendering the mail garbled.

To receive 8-bit character-encoded mail messages, you must disable the default conversion that postfix does. You use the command-line tool postconf to disable the setting.

1. Log in to your server as the administrator.
2. In Terminal, enter the following command:

```
sudo postconf -e disable_mime_output_conversion=yes
```

This will disable the special processing of Content-Type headers while delivering mail.

Mail Service Maintenance

2

After setting up Mail service you perform ongoing tasks to keep it running efficiently and smoothly. Server Admin has a number of features that help you with these day-to-day tasks.

This chapter describes the maintenance of basic Mail service, database, and the mail store, including archiving. It also contains information about mail monitoring, logging, and undeliverable mail.

Starting and Stopping Mail Service

Normally, Mail service is started after you complete the Server Assistant. You can also use Server Admin to start and stop Mail service.

You may not want to stop Mail service entirely, but instead hold outbound mail or block incoming mail connections. If you want to only partially disable Mail service, see the following:

- "Holding Outbound Mail" on page 56
- "Blocking Inbound Mail Connections" on page 56

You don't need to stop and start mail service to load settings into the mail software. If you want only new settings to take effect, see the following:

- "Reloading Mail Service" on page 56

To start or stop mail service:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Make sure at least one protocol (SMTP, POP, or IMAP) is enabled.
5. Click Start Service or Stop Service in the menu bar.

   When the service is turned on, the Stop Service button is available.

   If you plan to turn off Mail service for an extended period of time, notify users before you stop the service.

Holding Outbound Mail

You can prevent Mail service from sending outgoing mail. You might do this to isolate a problem or to prevent conflicts with another mail service running on your network. You might also do this to stop virus propagation or a spam relay originating with your server.

Holding mail isn't the same as disabling the SMTP service. Disabling prevents all user connections from sending outgoing mail, but holding outbound Mail service queues the mail for later sending. Mail is held in the outbound mail queue for inspection or deletion until you stop the hold.

To hold outbound mail:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click Hold Outbound Mail.
5. Click Save.

Blocking Inbound Mail Connections

You can prevent Mail service from receiving new inbound mail from external servers. You might do this to isolate a problem or to prevent conflicts with another mail service running on your network. You might also do this to stop virus propagation or a spam relay originating from external servers.

Blocking inbound mail isn't the same thing as disabling the SMTP service. Disabling prevents all queued mail from being sent out, but blocking inbound mail stops accepting connections to add mail to the queue. All attempted mail deliveries are bounced and returned to the sender.

To block inbound connections:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Deselect Allow Incoming Mail.
5. Click Save.

Reloading Mail Service

Sometimes it's necessary to reload the mail server for Mail service setting changes to take effect, for example, after restoring from backup, or altering the alias file. Reloading Mail service can be done without interrupting current mail service.

To reload Mail service:

1. Start Terminal.
2. As root, enter the following command:

```
postfix reload
```

Changing Protocol Settings for Incoming Mail

You can change the settings for incoming mail by choosing POP3, IMAP, or both:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Click the General tab.
4. Enable or disable the IMAP or POP checkbooks as needed.

Improving Performance

Mail service must act very fast for a short period of time. It sits idle until a user reads or sends a message, then it transfers the message immediately. Therefore, it puts intense but brief demands on the server.

As long as other services do not place heavy continuous demands on a server (for example, as a QuickTime streaming server would), the mail server can typically handle several hundred connected users.

As the number of connected mail users increases, the demand of Mail service on the server increases. If Mail service performance needs improvement, try the following:

- Adjust the load mail users can put on your server by limiting the number of mail connections. For instructions, see "Enabling IMAP Access" on page 25.
- Move the mail storage location to its own hard disk or hard disk partition. For instructions, see "Specifying the Location of the Mail Database and Mail Store" on page 59.
- Run other services on a different server, especially services that place frequent heavy demands on the server. (Each server requires a separate Mac OS X Server license.)

Working with the Mail Store and Database

The mail database keeps track of messages for mail service users. Mail service stores messages in separate files. You can do the following with the mail database and files:

- View and repair the mail store database.
- Repair user mail stores.
- Convert the mail database from an earlier version of Mac OS X Server.
- Specify where the mail database and files are stored.
- Backup and restore the mail store.

These tasks are described in this section.

Viewing the Location for the Mail Database and Mail Store

You can view the location of the mail store and database, as well as the size of the mail store. You may need to keep track of the current size of the mail store to plan mail server resources.

You do not change the location of the mail database or mail store here. To change their location, see "Specifying the Location of the Mail Database and Mail Store" on page 59.

To view the location of the mail store and database:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Maintenance.
3. Select the Database tab.

Repairing the Mail Database

If mail isn't making it to the correct user, or if messages aren't being sent properly, the mail database may be corrupted and need to be reconstructed. Mail service reads from its mailbox list database each time it tries to deliver a message to a user's inbox. Sometimes the mail server's mailbox list database can become corrupted.

Reconstructing a database can be done while the mail server is running. However, it is best to block incoming connections before recontructing, to make sure that incoming mail is processed using the fresh database. For instructions on blocking incoming connections, see "Blocking Inbound Mail Connections" on page 56.

To repair a corrupted mail server database:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Select the Database tab.
4. Click Repair.

Repairing the Mail User's Account Database

Mail service updates the user's database of stored messages each time a message is added, deleted, or moved. Sometimes during these updates, the mail store's database can become corrupted. When users report that mail messages have disappeared or become unreadable, the mail store database may be corrupted and need to be reconstructed. You repair a user's database when corruption is evident, and reconstruction only repairs the affected mailbox.

Reconstructing a database can be done while the mail server is running.

To reconstruct a corrupted mail database:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Select the Accounts tab.
4. Select the affected user's account.
5. Click Reconstruct.

Converting the Mail Store and Database from an Earlier Version

If you're upgrading Mac OS X Server from v10.1 or v10.2 to v10.5, you must migrate your mail store and database.

If you're upgrading from Mac OS X Server v10.3 or v10.4 you do not need to migrate your mail installation.

To convert the mail database, the server must have enough available disk space. The amount of available disk space should equal the size of the database file being converted. If there's not enough disk space available, Server Admin won't convert the mail database and messages.

To convert the mail store database:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Select the Migration tab.
4. Click Select and choose the location of the old Apple Mail Service database.

   By default the location for v10.1 and v10.2 was /Library/AppleMailServer.
5. Select the user account to migrate, and click Migrate User, or if you want to migrate all users, click Migrate All.

   Mail is exported to the default destination directory, creating target mailboxes as needed.

Specifying the Location of the Mail Database and Mail Store

If you're starting mail service for the first time and you have no existing mail database, you can specify where the mail database and message files will be stored. By default, the mail database location is /var/imap/ and the mail store location is /var/spool/imap/.

Note: Changing the mail store location of an existing mail system doesn't move the mail from the old location to the new one.

If this server is part of a mail server cluster, the mail store and database are kept on the Xsan cluster and their locations cannot be changed.

To specify where mail is stored on the server:

1. If Mail service is already running, stop the Mail service.

   See "Starting and Stopping Mail Service" on page 55.

   When mail service starts for the first time, it creates an empty mail store at the default location. You can ignore this or delete it after you specify an alternate mail storage location and restart mail service.
2. In Server Admin, select a computer in the Servers list, then select Mail.
3. Click Settings.
4. Click the Advanced tab.
5. Click Database.

   You'll see the current location of the mail database and the mail store.
6. In the Database Location field, enter the path of the location where you want the mail database to be stored.

   You can browse for a location by clicking Choose next to the Location field.
7. In the Mail Store Location field, enter the path of the location where you want the mail files to be stored.

   You can browse for a location by clicking Choose next to the Location field.

Creating Additional Mail Store Locations

Mail service can scale well as your storage needs change. You can spread the mail store across several disks or file systems. You can add new partitions to the mail store without requiring downtime, or even the users' knowledge.

To use new mail store locations, you designate the partition where the mail store resides. Enter the mail store path in the user's mail settings using Workgroup Manager. See *User Management* for more instructions.

The mail store partitions can be additional hard disk partitions or remotely mounted file systems. For remotely mounted file systems, NFS isn't recommended.

Note: Creating new locations doesn't automatically put mail in those locations. Edit the user records in Workgroup Manager to start delivering mail to the new partitions. Deleting a location doesn't delete the mail at that location, but makes those mail folders inaccessible.

To split the mail store:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Click the Advanced tab.
4. Click Database.

You'll see the current location of the mail database, and the mail store.

5 To add a location, click the Add (+) button below the Additional Mail Store Locations box and complete the following:

   a Enter a name for the mail store location (for example, "Marketing" or "Executive").

   b Enter the path to the new location (such as /Volumes/mailstore2).

   c Click OK.

6 To change a location, click the Edit (/) button below the Additional Mail Store Locations box.

   a Edit the path to the new location.

   b Click OK.

7 To remove a location, select the location to be deleted and click the Remove (–) button next to the Additional Mail Store Locations box.

8 Click Save.

Backing Up and Restoring Mail Messages

You can back up mail service data by making a copy of the Mail service folder. If you need to restore Mail service data, you can replace the Mail service folder with a backup copy.

You can back up individual mail storage folders, or the entire mail store, as needed. One command line tool that can be used to back up your mail messages is ditto. See ditto's man page for information.

Important: Stop mail service before backing up or restoring the Mail service folder. If you back up the Mail service folder while Mail service is active, the backup mail database file may go out of sync with the backup folder. If you restore the folder while Mail service is active, the active mail database file might go out of sync with the active folder.

An incremental backup of the Mail service folder can be fast and efficient. If you back up your mail data incrementally, the only files copied are the small database file and the message files that are new or changed since the last backup.

After restoring the Mail service folder, notify users that messages stored on the server have been restored from a backup copy.

An excellent source for information on backing up mail messages can be found at: acs-wiki.andrew.cmu.edu/twiki/bin/view/Cyrus/Backup

Setting Up Mail Server Clustering

With Xsan, you can cluster multple mail servers that share the mail store and database. This provides mission-critical redundancy and high-performance and allows you to easily maintain the pooled storage using Xsan tools and software.

With mail server clustering, a single mail store is used by every member of the cluster. Each member, also called a *node*, maintains its own mail database, which are also stored on the Xsan cluster.

Each server also has a primary SMTP spool file. If a server goes offline, another node in the cluster takes over processing of the failed sever's spool file. This happens automatically, but you will see it noted in the log files.

You can configure your mail server to join an existing mail cluster as a new member of the cluster, or you can migrate a mail server's mail store and database to another server that is a member of the cluster.

If you have Xsan software installed, you can also create a cluster, with the current server becoming the cluster's first member.

Configuring Mail Clustering

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Advanced.
3. Click Clustering.
4. Click the Change button, then follow the onscreen instructions that appear.

Note: After a server has joined a cluster changes to mail server settings, such as SMTP, POP, IMAP, and logging, will affect all servers in the cluster.

When you remove the last member of a cluster, you must designate a server to take over as a standard mail server.

Monitoring Mail Messages and Folders

This section describes how to perform common administrator tasks for monitoring mail messages.

Allowing Administrator Access to Mail Folders

You can configure IMAP to allow the server administrator to view the mail service hierarchy. Administrators cannot view mail itself, only users folder locations.

When you connect as the IMAP administrator, you see user mail folders stored on the server. Each user's mailbox appears as a separate folder in your mail client. You can remove inactive mailbox folders that belong to deleted user accounts.

To configure administrator access to mail folders:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab and select Enable IMAP, if it isn't selected.
4. Select an existing user or create a new user using Workgroup Manger to be an IMAP administrator.
5. If you haven't created a user record for the mail administrator's account, see *User Management*.
6. Open /etc/imapd.conf in a text editor.

   If you aren't comfortable using a Terminal-based text editor like emacs or vi, you can use TextEdit.
7. Find the line that reads "admins:"
8. Edit the line to add the UID number of the administrator account after the colon.
9. Save your changes.
10. In your mail client application, create an account that uses IMAP to connect to your mail service using the mail administrator name.

    For more information, see the man page for imapd.conf.

Saving Mail Messages for Monitoring and Archival Purposes

You can configure mail service to send a blind carbon copy (Bcc) of each incoming or outgoing message to a user or group that you specify. You might want to do this if you need to monitor or archive messages. Senders and receivers of mail don't know that copies of their mail are being archived.

You can set up the specified user or group to receive blind carbon copies using POP, then set up a client mail application to log in periodically and clean out the account by retrieving all new messages. Otherwise, you may want to periodically copy and archive the messages directly from the destination directory with automated shell commands. You can set up filters in the mail client to highlight certain types of messages. Additionally, you can archive all messages for legal reasons.

To save all messages:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the General tab.
4. Click the "Copy all mail to" checkbox and enter a user name or group name.
5. Click Save.

Monitoring Mail Service

This section describes how to use Server Admin to monitor overall mail server activity, logs, and connected mail users. This section also describes how Mac OS X Server reclaims disk space used by logs and how you can reclaim space manually.

Viewing Mail Service Activity

You can use Server Admin to see an overview of Mail service activity. The overview reports whether the service is running, when Mail service started, and incoming and outgoing connections by protocol.

To see an overview of Mail service activity:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Overview button.

Viewing the Mail Connections List

Server Admin can list the users who are connected to the mail service. For each user, you see the user name, IP address of the client computer, type of mail account (IMAP or POP), number of connections, and connection length.

To view a list of connected mail users:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Connections button.

Checking the Outgoing Mail Queue

You may need to check mail that is waiting to be sent. If you have a message backlog, or if you have interrupted outbound mail, you may have a number of items in the queue. Additionally, you may want to monitor mail delivery to ensure that mail is being delivered to both local and remote hosts.

When checking the queue, you see the message ID number, sender, recipients, date, and message size. You can select a message in the queue and inspect the message headers.

To check the outgoing mail queue:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Click the Mail Queue tab.
4. To inspect amessage, select it.

Clearing Messages from the Outgoing Mail Queue

Your outgoing mail queue may have a backlog of messages. These are messages that can't be sent for any number of reasons: the message might be improperly addressed, the destination server might be unresponsive, or the destination account may be over quota. In such circumstances, you may want to clear messages from the queue backlog.

To clear a message from the outgoing queue:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Click the Mail Queue tab.
4. Select the message to be deleted.
5. Click Delete.

Viewing Mail Accounts

You can use Server Admin to see a list of users who have used their mail accounts at least once. For each account, you see the user name, disk space quota, disk space used, and percentage of space available to the user.

Mail accounts that have never been used aren't listed.

To view a list of mail accounts:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Maintenance.
3. Click the Accounts button.

Viewing Mail Service Logs

Mail service maintains the following logs that you can view in Server Admin. The file location for each log is shown beneath the Show pop-up menu.

- *Mail Access:* General mail service information goes into this log.
- *IMAP log:* IMAP-specific activity goes into this log.
- *POP log:* POP specific activity goes into this log.
- *SMTP log:* SMTP specific activity goes into this log.
- *Mailing List logs:* The logs record Mailmain's activity, including service, error, delivery failures, postings, and subscriptions.
- *Junk Mail and Virus logs:* These show activity for mail filtering, including logs for virus definition updates (freshclam log), virus scanning (clamav log), and mail filtering (amavis log).

Logs can be refined by using the text filter box in the window.

To view a mail service log:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click the Logs button.
3. Choose a log type from the View pop-up menu.
4. Click Save.

Setting Mail Service Log Detail Level

Mail service logs can show the folowing levels of reported detail:

- Low (errors only)
- Medium (errors and messages)
- High (all events)

You can choose log detail for each service category (outgoing, incoming, or junk mail filter).

To set the mail service log detail:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Logging tab.
4. Select the Service whose log detail you want to set.
   - SMTP for outgoing mail and connections from external mail servers.
   - POP/IMAP for incoming mail retrieval for users.
   - Junk Mail/Virus for the junk mail service.
5. Choose a detail level from the Log Detail Level pop-up menu.
6. Click Save.

Archiving Mail Service Logs by Schedule

Mac OS X Server archives Mail service logs after a specified amount of time. Each archive log is compressed and uses less disk space than the original log file. You can customize the schedule to archive the logs after a set period of time, measured in days.

To archive logs by schedule:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Logging tab.
4. Click "Archive Logs Every ____ Days."
5. Enter the number of days.
6. Click Save.

Reclaiming Disk Space Used by Mail Service Log Archives

Mac OS X Server reclaims disk space used by mail service logs when they reach a specified size or age. If you're comfortable using the Terminal application and UNIX command-line tools, you can use the command-line tool diskspacemonitor to monitor disk space when you want, and delete or move the log archives. For additional information, see diskspacemonitor in *Command-line Administration*.

When a Disk Is Full

Mail services become erratic and suffer from data corruption if the disk storing your mail reaches maximum capacity. When your disk reaches full capacity, you'll experience the following:

- **Postfix:** If the operating system can still spawn the smtpd process, Postfix will try to function and attempt to accept the message. The message will then be rejected with a "disk full" error. Otherwise, its behavior is unpredictable.
- **Cyrus:** If the operating system can still spawn an imapd or pop3d process, the server will attempt to open the user's mail account. Upon success, the user can access mail as normal. Any changes that require database additions and causing the database to grow can cause the process to hang and corrupt the database.

When Mail Is Undeliverable

Mail messages might be undeliverable for several reasons. Incoming mail might be undeliverable because it has a misspelled address or is addressed to a deleted user account. Outgoing mail might be undeliverable because it's misaddressed or the destination mail server isn't working. You can configure your mail service to:

- Forward undeliverable incoming mail
- Limit the number of attempts to deliver problematic outgoing mail
- Report failed delivery attempts
- Use a different timeout value to increase the chance of connection success

Forwarding Undeliverable Incoming Mail

You can have mail service forward messages that arrive for unknown local users to another real local person or a group in your organization. Whoever receives forwarded mail that's incorrectly addressed (with a typo in the address, for example) can forward it to the correct recipient.

If forwarding of these undeliverable messages isn't explicitly enabled, the messages are returned to sender.

To set up forwarding of undeliverable incoming mail:

1 Open /etc/postfix/main.cf in a text editor.

If you aren't comfortable using a Terminal-based text editor like emacs or vi, you can use TextEdit.

2 Find the line that reads "luser_relay."

3 Remove the hash character ("#") at the beginning of the line, if present.

4 Edit the line to add the user name, alias, or group of the destination account after the equal sign ("=").

5 Save your changes.

6 Reload the mail server.

For more information about reloading Postfix, see "Reloading Mail Service" on page 56.

Copying Undeliverable Incoming Mail

You can have mail service copy messages that arrive for unknown local users to another person or a group in your organization, usually the postmaster. You can use this setting to keep track of mail delivery failures such as SMTP connection rejections, misaddressed mail or determining the source of junk mail

To keep a copy of undeliverable incoming mail:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the General tab.

4 Select "Copy undeliverable mail to" and enter a user, group name, or alias.

5 Click Save.

Retrying Undelivered Outgoing Messages

Sometimes the outgoing mail queue has undelivered messages. These messages are properly addressed, but for some reason (for example, the destination server is down, or the firewall is blocking the outgoing port for SMTP) the messages aren't sent.

You can attempt to send the messages again. Normally, the mail server attempts to retry sending by itself, but you can trigger it manually instead of waiting.

To try to send an outgoing message again:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Maintenance.

3 Click the Mail Queue tab.

4 Select the message to retry sending.

Hold down the shift key or the command key to select more than one message.

5 Click Retry.

Where to Find More Information

You can find more information about Mail service in books and on the Internet.

Books

For general information about mail protocols and other technologies, see these books:

- A good introduction to mail service can be found in *Internet Messaging,* by David Strom and Marshall T. Rose (Prentice Hall, 1998).
- For more information about MX records, see "DNS and Electronic Mail" in *DNS and BIND,* 3rd edition, by Paul Albitz, Cricket Liu, and Mike Loukides (O'Reilly and Associates, 1998).
- Also of interest is *Removing the Spam: Email Processing and Filtering,* by Geoff Mulligan (Addison-Wesley Networking Basics Series, 1999).
- To learn about mail standards, see *Essential email Standards: RFCs and Protocols Made Practical,* by Pete Loshin (John Wiley & Sons, 1999).
- To learn more about Postfix, see *Postfix*, by Richard Blum (Sams; 1st edition, 2001)
- To learn more about Cyrus, see *Managing IMAP,* by Dianna Mullet, Kevin Mullet (O'Reilly & Associates, 2000)

Internet

There is an abundance of information about the different mail protocols, DNS, and other related topics on the Internet.

An overview of mail systems can be found at this website:
www.wikipedia.org

Request for Comments (RFC) documents provide an overview of a protocol or service and details about how the protocol should behave. If you're a novice server administrator, you may find some of the RFC background information helpful. If you're an experienced server administrator, you'll find all the technical details about a protocol in its RFC document. You can search for RFC documents by number at this website:
www.faqs.org/rfcs

For technical details about how mail protocols work, see these RFC documents:

- *POP:* RFC 1725
- *IMAP:* RFC 2060
- *SMTP:* RFC 821 and RFC 822
- *Sieve:* RFC 3028

For more information about Postfix, go to:
www.postfix.org

For more information about Cyrus, go to:
asg.web.cmu.edu/cyrus

For more information about Sendmail, go to:
www.sendmail.org

For more information about SquirrelMail, go to:
www.squirrelmail.org

For more information about Sieve, go to:
www.cyrusoft.com/sieve

For more information about servers that filter junk mail:
www.ordb.org

Mailing Lists

3

Mac OS X Server provides two types of mailing lists. A Mailman-based list where a single mail message is distributed to recipients who have subscribed to the list, and a group-based list which allows you to send a single message which is copied to each individual member a workgroup.

Mailman-based Mailing Lists

Mac OS X Server uses Mailman for its traditional mailing list service. Mailing lists differ from workgroups in a few fundamental ways:

- Mailing lists aren't linked to file or directory permissions.
- Mailing lists can be administered by someone other than the workgroup or server administrator.
- Mailing list subscribers do not need an account (mail or file access) on the list's server; any mail address can be added to the list.
- Mailing list subscribers can often remove themselves from and add themselves to lists.

Group-based Mailing Lists

A group mailing list is based on a directory group. It differs from a Mailman-based mailing list in the following ways:

- Group members receive all messages sent to the group's address. No subscription is required.
- The recipients list is up-to-date with the directory group, so only members of the group receive mail messages.
- The group administrator controls the membership of the group.

Setting Up a Groups-based Mailing List

If you want to send mail messages to all members of a group, you can enable server group mailing lists. Each individual member of the directory group receives a copy of messages sent to the group address.

To enable groups-based mailing lists:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click Enable Server Group Mailing Lists.
5. Enter an interval for how frequently the recipients list is updated.

   The mail server rescans the group membership periodically, members added to the group between updates of the recipients list won't receive any messages until the mail server reads the group membership record.
6. In Workgroup Manager, enable the Mailing List service for each group you want to have a mailing list address.

   The setting is located in the Basic group options in Workgroup Manager.

   See *Open Directory Administration* for information about using Workgroup Manager.

Note: The address for a group-based list is *group_shortname@ServerDNSname*.

Some of Mailman's main features include (from www.list.org/features.html):

- Web-based list administration for nearly all tasks, including list configuration, moderation (post approvals), management of user accounts.
- Web-based subscribing and unsubscribing, and user configuration management. Users can temporarily disable their accounts, select digest modes, hide their mail addresses from other members, and so on.
- A customizable home page for each mailing list.
- Per-list privacy features, such as closed-subscriptions, private archives, private membership rosters, and sender-based posting rules.
- Configurable (per-list and per-user) delivery mode.
- Integrated bounce detection within an extensible framework.
- Automatic disposition of bouncing addresses (disable, unsubscribe).
- Integrated spam filters.
- Built-in web-based archiving, with hooks for external archivers.
- Integrated Usenet gatewaying.
- Integrated autoreplies.
- Majordomo-style mail-based commands.
- Multiple list owners and moderators.

- Support for virtual domains.
- Compatibility with most web servers and browsers, and most SMTP servers. Requires Python 2.1.3 or later.
- An extensible mail delivery pipeline.
- High-performance mail delivery, with a scalable architecture.

For more information about Mailman see:
www.list.org

Setting Up a Mailman Mailing List

This section describes the process of setting up a Mailman mailing list. To do this, you enable the service, define a list name, and add subscribers to the list.

When you create a mailing list, you must specify a master password that gives you control over all lists. Do not use an administrator's or user's login password. You must also specify the mail addresses of other administrators who need the master password. The following topics explain how to set up a mailing list:

Enabling Mailing Lists

Before you can define mailing lists and subscribers, you must enable the list service and create the administrator's default mailing list. When you enable mailing lists, you also create a password that allows administration of all lists on the server and automatically create a special list for mailing list administrators. Mailing list administrators get a copy of the master list password and error notifications.

Note: This list (called Mailman) must exist for mailing lists to function correctly. Do not remove the master list.

To enable mailing lists:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click Enable Mailman Mailing Lists.
5. Enter the master list password.
6. Enter the mail addresses of the list administrators, then click OK.

   You must enter at least one administrator who will receive notifications about the mailing list service.
7. Click Save.

   The Mailman list is created and the master password sent to the indicated administrators.

Creating a Mailing List

Mailing lists distribute a single mail message to multiple recipients. After you create a mailing list, any mail sent to the list's address is sent to all subscribers. Mailing lists have list administrators who can change list membership and list features.
Lists can be self-subscribing, so list administrator's don't need to add and remove subscribers; the subscribers can do so themselves.

Note: Mailing lists cannot be renamed or corrected after creation. This is a limitation of Mailman, the list software used by Mac OS X Server. Although you can change the case of a list name, using Mailman's own web interface, Server Admin doesn't allow changing the list name in any way.

To rename or correct a list name, you must create a new list and add the existing users to the new list. This will result in a Welcome message to be sent to all listed users.

To create a list:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click the Add (+) button under the Lists pane.
5. Enter the list's name.

   The list name is the mail account name to which mailing list users will send their mail. The name isn't case-sensitive, and cannot contain spaces.
6. Enter the list administrator's mail address, then click Edit.

   If you only enter a name, it must be a username on the server. If you enter a username@domain, the administrator doesn't need to be a local user.
7. Click Users May Self Subscribe, if desired.
8. Choose the default language for the list.

   You can choose English, German, Japanese, Korean, Russian, or Spanish. This setting encodes the text generated by the list appropriately for the default language.
9. Choose additional languages you want to be supported by the list.

   This setting also encodes the text generated by the list appropriately for the default language.
10. Click OK.
11. Click Save.

You can now add subscribers to the list. See "Adding Subscribers" on page 78.

If you have allowed users to self-subscribe, they can subscribe using mail or the web administration page.

Setting a List's Maximum Message Length

You can set the maximum size message that the list accepts. You can disallow large attachments by setting a small maximum size, or you can allow file collaboration by setting an unlimited message size.

You use Server Admin to set the maximum message length.

To set a list's maximum message length:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list whose message length you want to set.
5. Click the Edit (/) button under the Lists pane.
6. Enter the maximum message length (in KB).

   If you enter 0, the maximum length is unlimited.
7. Click OK.

Creating a Mailing List Description

Sometimes it's difficult to know the scope and subject matter of a mailing list from the short list name. The list information page contains a description of the list, what subject matter it covers, and can include who is permitted to subscribe. These details are especially good for self-subscription lists. A potential subscriber can decide whether to subscribe from the list's description.

You use the web interface to set the mailing list description. Web services must be enabled to access the web-based interface.

To create a list description:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   server.domain.tld/mailman/admin/*listname*
2. Enter the master list password and click "Let me in."

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.
3. Make sure that General Options is selected from the Configuration Categories link section.
4. Enter a short phrase in the description text box.
5. Enter a few paragraphs about the list, its rules, and its content expectations in the info text box.

6 Click Submit Your Changes.

Customizing the Mailing List Welcome Message

When subscribers join a mailing list, either by assignment or self-subscription, they receive an automated welcome message. The message explains where to find the list archives and how to unsubscribe. You can customize it by adding additional text, describing the list culture and rules, or any other information you want subscribers to have.

You use the web interface to set the mailing list welcome message. Web services must be enabled to access the web-based interface.

To customize a welcome message:

1 In a web browser, enter the URL of the list administration page. This is usually: *server.domain.tld*/mailman/admin/*listname*

2 Enter the master list password.

This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.

3 Make sure that General Options is selected from the Configuration Categories link section.

4 Enable "Send welcome message to newly subscribed members."

5 Enter the text you want to include in the "List-specific text prepended..." text box.

6 Click Submit Your Changes.

Customizing the Mailing List Unsubscribe Message

When a user unsubscribes from a mailing list, either by the list administrator or by directly unsubscribing, the user receives an automated unsubscribe message. The message confirms the unsubscribing. You can customize it by adding any information you want users to have upon leaving the list.

You use the web interface to set the mailing list welcome message. Web services must be enabled to access the web-based interface.

To customize the subscriber welcome message:

1 In a web browser, enter the URL of the list administration page.

This is usually *server.domain.tld*/mailman/admin/*listname*.

2 Enter the master list password.

This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.

3 Make sure that General Options is selected from the Configuration Categories link section.

4 Enable "Send goodbye message to members."

5 Enter the text you want to include in the "Text sent to people leaving the list" text box.

6 Click Submit Your Changes.

Enabling a Mailing List Moderator

You can create a moderated list where the posts must be approved by a list administrator before the post is sent. You designate list moderators, who have limited administrative privileges. They can't change list options, but they can approve or reject subscription requests and postings.

When moderators enter their password in the list administration page, they get a page with their own moderating tasks available.

You use the web interface to set mailing list moderation. Web services must be enabled to access the web-based interface.

To enable list moderation:

1 In a web browser, enter the URL of the list administration page.

This is usually *server.domain.tld*/mailman/admin/*listname*.

2 Enter the master list password.

This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to list administrators designated at that time.

3 Make sure that General Options is selected from the Configuration Categories link section.

4 Enter the list moderator addresses you want to include in the "The list moderator mail addresses" text box.

5 Click Submit Your Changes.

6 Select the Password Options in the Configuration Categories link section.

7 Enter a password in the moderator password field, and confirm it.

8 Click Submit Your Changes.

Setting Mailing List Message Bounce Options

When a list message bounces and returns to the list server, you can choose how the list server handles the resulting bounce message.

You use the web interface to set the mailing list bounce options. Web services must be enabled to access the web-based interface.

To set bounce options:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   server.domain.tld/mailman/admin/*listname*

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server, and mailed to all the list administrators designated at that time.

3. Select Bounce Processing in the Configuration Categories link section.

4. Select the bounce processing options you want.

   Each option section has a link to a help page which explains the option setting.

5. Click Submit Your Changes.

Designating a Mailing List as Private

You may not want to show certain lists on the web list access page. You can designate a list as "private" so it isn't shown at:
server.domain.tld/mailman/listinfo

You use the web-based interface to set a list's privacy options. Web services must be enabled to access the web-based interface.

To set privacy options:

1. In a web browser, enter the URL of the list administration page.

   This is usually *server.domain.tld*/mailman/admin/*listname*

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.

3. Select Privacy Options then Subscription Rules in the Configuration Categories link section.

4. Deselect "Advertise this list..." in the privacy list.

5. Click Submit Your Changes.

Adding Subscribers

Use Server Admin to add mailing list subscribers to a list. Mailing list subscribers do not need an account (mail or file access) on the list's server. Any mail address can be added to the list. You must have an existing list to add a subscriber.

If the subscriber is a user on the mail server, you can use the Users and Groups button to add a local subscriber to the list.

To add subscribers:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list you want to add a subscriber to.
5. Click the Add (+) button under the Members pane.
6. Enter the recipient's mail address.

   If you're entering multiple subscribers, enter the recipient mail addresses or drop a text list into the User Identifiers box.

   If the subscribers are users on the mail server, you can use the Users and Groups button to add a local groups to the list.
7. Assign the subscriber privileges:
   - ***Users subscribed to list:*** This means the user will receive mail sent to the list address.
   - ***Users may post to list:*** This means the list will accept mail from the user.
   - ***Users can administer list:*** This means the user has administrative privileges for the list.
8. Click OK.

Administering Mailing Lists

Mailing lists can be administered by a designated list member, called list administrators, or list managers. List can add or remove subscribers, and can designate other list administrators. List administrators can also designate list moderators, who have limited administrative privileges. They can't change list options, but they can approve or reject subscription requests and postings.

Mailman uses a web interface as well as mail-based administration. Web services must be enabled to access the web interface. Dozens of configuration options are available for Mailman mailing lists that are not accessible using Server Admin.

The Web-based administration interface is found at:
server.domain.tld/mailman/listinfo

Information and access to a specific list is found at:
server.domain.tld/mailman/listinfo/*listname*

For documentation of these functions for users, list administrators, and server administrators, see:
www.list.org/docs.html

Viewing a Server's Mailing Lists

You can view public (not private) lists that are being run on a server through the server's web information portal. Web services must be enabled to access the portal.

To see the lists:

- Open a web browser, and enter the list's URL:
  server.domain.tld/mailman/listinfo

Viewing a Mailing List's Information Page

Each list has an information page on the server that shows basic information about the list, how to post to it, how to subscribe to it, and how to access your own subscription preferences. You access the list information page with a web browser.

Web services must be enabled to access the web interface.

To see the list's information page:

- Open a web browser, and enter the list's URL:
  server.domain.tld/mailman/listinfo/*listname*

Designating a List Administrator

When you set up a mailing list, you designate at least one user to administer it. This administrator has access to the other list settings pages for all lists on the server.

You can designate more than one list administrator and change any subscriber to or from being a list administrator. You can add remove or change the list administrator using these instructions.

List administrators do not need to be users (neither administrator nor regular) on the server. They are listed as mail addresses. Giving list administrator privileges to a subscriber does not give them any privileges on the mailing list server other than making and removing lists and editing list preferences.

To designate a list administrator:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list that has the subscriber to be given list administrator privileges.

   If the user isn't already subscribed to the list, you'll have to add him or her first. See "Adding Subscribers" on page 78 for more information.
5. Select the subscriber.
6. Click the Admin checkbox in the subscriber list, if desired.
7. Click OK.

Accessing Web-based Administrator Options

List administrators set preferences for mailing list behavior. They also view pending moderation requests for mailing lists that are being run on a server. These tasks and many more are accomplished through the server's web-administration portal. Web services must be enabled to access the web portal.

Server Admin does not give access to the wide range of preferences available for a mailing list. List administrators are encouraged to use the web interface for all but the most basic setup tasks.

Information about what options are available via the web interface can be found at: www.list.org/docs.html

To access a list's web-based options:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   server.domain.tld/mailman/admin/*listname*

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.

3. Change list settings as desired.

Designating a List Moderator

When you set up a list, you can designate another user to moderate the list.

To designate a list moderator:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list that has the desired subscriber.
5. Click the Edit (/) button under the Lists pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Select or deselect "User can administer the list" as necessary.
7. Click OK.

Archiving a List's Mail

Messages sent to a mailing list can be archived and viewed at a later time. The messages are grouped into archival volumes by time and date. You can choose whether a list's archive is accessible by nonsubscribers, and how often the archives are updated.

By default, the archives are found at:
server.domain.tld/pipermail/*listname*

You use the web-based interface to set the mailing list archive preferences. Web services must be enabled to access the web-based interface.

To archive a list's mail:

1. In a web browser, enter the URL of the list administration page.

   This is usually:
   server.domain.tld/mailman/admin/*listname*

2. Enter the master list password.

   This is not the user's login password. The master list password was set when mailing lists were enabled on the server. It was mailed to list administrators designated at that time.

3. Select "Archiving Options" from the Configuration Categories section.
4. Select Yes next to "Archive messages?"
5. Select whether the archive will be public or private.
6. Select how often to start a new archive volume.
7. Click Submit Your Changes.

Viewing Mailing List Archives

If the list administrator has enabled message archiving, you can access and search the archived messages.

To view a list's archives:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/archives/*listname*

2. Select the year and month of the archive you'd like to browse.

Working with Mailing List Subscribers

After a mailing list is created, you can add or remove people from it. You may want to give list administration privileges to a user or change a user's ability to receive or post to the list.

Adding a Subscriber to a List

This is the same procedure as adding a user to a new list.

To add a subscriber to a list:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the List to add a subscriber to.
5. Click the Add (+) button under the Members pane.
6. Enter the recipient's mail address.

   The mail address must match the return address of the recipient to post messages without administrator approval.

   If a user was added via the Users and Groups button, the mail address in the list is in the form of user@server.domain.com. If necessary, change the mail address in the mailing lists panel of Server Admin to match the return address used by the client.
7. Assign the subscriber privileges.
8. Click OK.

Removing a List Subscriber

You can remove a subscriber from a mailing list, either forcibly or by request.

To remove a list subscriber:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list you want to remove a subscriber from.
5. Select the subscriber from the User pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Click the Remove (–) button under the Email Address pane.

Changing Subscribers Posting Privileges

Sometimes you may want an announce only list, where recipients can't post to the address. You can limit the ability of subscribers to post and create an announce-only list.

To add or remove a subscriber's posting privileges:

1. In Server Admin, select a computer in the Servers list, then select Mail.
2. Click Settings.
3. Select the Mailing Lists tab.

4 Select the list that has the desired subscriber.

5 Click the Edit (/) button under the Mailing Lists pane.

Hold down the Shift or Command key to select multiple subscribers.

6 Select or deselect the Post checkbox as necessary.

This setting determines whether or not the user can send messages to the list.

7 Click OK.

Suspending a Subscriber

You can keep a user on a mail list and still allow him or her to post to a list without receiving list messages. In this case, you temporarily suspend a user's subscription to a list.

To suspend a user's subscription to a list:

1 In Server Admin, select a computer in the Servers list, then select Mail.

2 Click Settings.

3 Select the Mailing Lists tab.

4 Select the List that has the desired subscriber.

5 Click the Edit (/) button under the Mailing Lists pane.

Hold down the Shift or Command key to select multiple subscribers.

6 Deselect or select "Subscribe" as necessary.

7 Click OK.

List Subscriber Options

A subscriber can customize certain aspects of their mailing list subscriptions. Without being designated a list administrator or having any user privileges on the server, the user has control of a number of aspects of his or her subscriptions.

The following section gives instructions on a few common settings your users can customize. A full list of possible configurable options, and instructions for use can be found on Mailman's documentation page at:
www.list.org/docs.html

Subscribing to a Mailing List Via Mail

You can subscribe to lists using mail. You do so by sending a message to the list subscription address. Depending on the list's settings, you may need to confirm your subscription or wait for moderator approval. You do not need to subscribe using both mail and the web. Just one will suffice.

If the list allows self-subscription, you can subscribe yourself.

To subscribe via mail:

1. Open your mail program that sends from the address you want to subscribe.
2. Send a message to the list subscription address, which is usually:

   listname-join@*domain*

   The subject and body of the message will be ignored. Replace listname with the name of the list and the domain where the list is hosted.

Subscribing to a Mailing List Via Web

You can subscribe to lists using the web interface. You go to the information page for the list and provide your mail address and a password for your list preferences. Depending on the list's settings, you may need to confirm your subscription or wait for moderator approval. You do not have to subscribe using both the web and mail. Just one will suffice.

You can subscribe only yourself, if the list allows self-subscription.

To subscribe via web:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/listinfo/*listname*
2. In the Subscriber section of the web page, enter your mail address and name (the name is optional).
3. Specify a password for use with the list, and enter it twice to confirm it.

   This should not be a login password, or used for any other purpose than for list option administration. It is occasionally mailed to you in plain text.
4. Select your digest message mode preference.

   If you receive a daily digest, instead of getting each list posting separately, you will get one daily post.
5. Click Subscribe.

Unsubscribing from a Mailing List Via Mail

Unsubscribing from a mailing list is a similar process to subscribing to a mailing list via mail. Depending on the list's settings, you may need to confirm your subscription removal or wait for moderator response.

To unsubscribe via mail:

1. Open your mail program that sends from the address that receives the mailing list posts.

2 Send a mail message to the list subscription address, which will is usually:

listname-leave@*domain*

The subject and body of the message are ignored. Substitute listname with the name of the mailing list.

3 Follow the directions in the confirmation mail.

Unsubscribing from a Mailing List Via Web

Unsubscribing from a mailing list via the web is a similar process to subscribing to a mailing list via the web. Depending on the list's settings, you may have to confirm your subscription removal or wait for moderator response.

To unsubscribe via web:

1 In a web browser, enter the URL of the list information page.

This is usually:
server.domain.tld/mailman/listinfo/*listname*

2 In the Subscriber section of the web page, enter your mail address and click Unsubscribe Or Edit Options.

3 Click Unsubscribe.

Setting and Changing Your Mailing List Password

You use your mailing list password to alter preferences for a list. The password should not be one that you use for other purposes because it is sent in plain text as a reminder periodically from the lists you are subscribed to.

To setting or change your password:

1 In a web browser, enter the URL of the list information page.

This is usually:
server.domain.tld/mailman/listinfo/*listname*

2 In the Subscriber section of the web page, enter your mail address, and click Unsubscribe Or Edit Options.

3 Enter your password, and click Log In.

This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via mail or were subscribed via Server Admin, your password is blank.

4 Find the password section of the subscription page.

5 Enter a new password in the indicated field, and enter it again to confirm it.

To change your password for all lists that you belong to on this server, select Change Globally.

6 Click Change My Password.

Disabling List Mail Delivery

You can temporarily disable delivery of mailing list messages. (For example, to avoid excess mail while on vacation.)

To disable list delivery:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/listinfo/*listname*

2. In the Subscriber section of the web page, enter your mail address, and click Unsubscribe Or Edit Options.

3. Enter your password, and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via mail or were subscribed via Server Admin, your password is blank.

4. In the Mail Delivery section, select Disabled.

   To disable delivery for all lists that you belong to on this server, select Change Globally.

5. Click Submit My Changes.

Changing Digest Mode

Digest mode sends only one message per day regardless of list mail volume. You can switch between getting each message or a single digest message.

If your digest mode is *On* you receive a single digest message per day.

To toggle digest mode:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/listinfo/*listname*

2. In the Subscriber section of the web page, enter your mail address and click Unsubscribe Or Edit Options.

3. Enter your password and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via mail or were subscribed via Server Admin, your password is blank.

4. In the Set Digest Mode section, select whether you want a daily digest by clicking On or Off.

5. Click Submit My Changes.

Choosing MIME or Plain Text Digests

If you subscribe to a mailing list and receive digests (a single mail with all of a day's postings in it), you can choose whether to receive them as a MIME digest (a collection of individual posts) or as a plain text digest (one message with the text of all posts).

To change message types:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/listinfo/*listname*

2. In the Subscriber section of the web page, enter your mail address, and click Unsubscribe Or Edit Options.

3. Enter your password and click Log In.

   This is not your user password. If you subscribed using the web interface, you chose a list password. If you subscribed via mail or were subscribed via Server Admin, your password is blank.

4. In the Get MIME Or Plain Text Digests section, select a digest type.

   To set the digest type for all lists you belong to on this server, select Change Globally.

5. Click Submit My Changes.

Setting Additional Subscriber Options

Subscribers can change other list membership options, including their:

- Mail address
- Name on the list
- Posting acknowledgments
- Message copy handling

These options are available on your subscription options page.

To access additional options:

1. In a web browser, enter the URL of the list information page.

   This is usually:
   server.domain.tld/mailman/listinfo/*listname*

2. In the Subscriber section of the web page, enter your mail address, and click Unsubscribe Or Edit Options.

3. Find the option you want to change and follow the instructions on screen.

Where to Find More Information

Mailman's features and its capabilities, can be found at:
www.list.org

You will also find the following information at www.list.org/docs.html:

- Web-based administration and subscriber commands
- Mail-based administration and subscriber commands
- Frequently Asked Questions (FAQ) lists

Glossary

This glossary defines terms and spells out abbreviations you may encounter while working with online help or other Mac OS X Server Documentation. References to terms defined elsewhere in the glossary appear in *italics*.

access control A method of controlling which computers can access a network or network services.

access control list See **ACL**.

access privileges See **permissions**.

ACL A list maintained by a system that defines the rights of users and groups to access resources on the system.

address A number or other identifier that uniquely identifies a computer on a network, a block of data stored on a disk, or a location in a computer memory. See also **IP address**, **MAC address**.

alias Another email address at your domain that redirects incoming email to an existing user.

alphanumeric Containing characters that include letters, numbers, and punctuation characters (such as _ and ?).

APOP authentication An extension to the POP3 mail protocol. It ensures that the username and password are encrypted before being used to authenticate to a mail server.

authentication The process of proving a user's identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user's level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

back up (verb) The act of creating a backup.

backup (noun) A collection of data that's stored for purposes of recovery in case the original copy of data is lost or becomes inaccessible.

bit A single piece of information, with a value of either 0 or 1.

byte A basic unit of measure for data, equal to eight bits (or binary digits).

canonical name The "real" name of a server when you've given it a "nickname" or alias. For example, mail.apple.com might have a canonical name of MailSrv473.apple.com.

certificate Sometimes called an "identity certificate" or "public key certificate." A file in a specific format (Mac OS X Server uses the x.509 format) that contains the public key half of a public-private keypair, the user's identity information such as name and contact information, and the digital signature or either a *Certificate Authority* (CA) or the key user.

Certificate Authority An authority that issues and manages digital certificates in order to ensure secure transmission of data on a public network. See also **public key infrastructure** and **certificate**.

certification authority See **Certificate Authority**.

character A synonym for byte.

cleartext Data that hasn't been encrypted.

client A computer (or a user of the computer) that requests data or services from another computer, or server.

command line The text you type at a shell prompt when using a command-line interface.

command-line interface A way of interfacing with the computer (for example, to run programs or modify file system permissions) by entering text commands at a shell prompt.

computer name The default name used for SLP and SMB/CIFS service registrations. The Network Browser in the Finder uses SLP to find computers advertising Personal File Sharing and Windows File Sharing. It can be set to bridge subnets depending on the network router settings. When you turn on Personal File Sharing, users see the computer name in the Connect To Server dialog in the Finder. Initially it is "<first created user>'s Computer" (for example, "John's Computer") but can be changed to anything. The computer name is used for browsing for network file servers, print queues, Bluetooth discovery, Apple Remote Desktop clients, and any other network resource that identifies computers by computer name rather than network address. The computer name is also the basis for the default *local hostname*.

cracker A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to hacker.

decryption The process of retrieving encrypted data using some sort of special knowledge. See also **encryption**.

digital signature An electronic signature that can be used to verify the identity of the sender of a message.

directory Also known as a folder. A hierarchically organized list of files and/or other directories.

directory services Services that provide system software and applications with uniform access to directory domains and other sources of information about users and resources.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

DNS domain A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

DNS name A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

domain name See **DNS name**.

Domain Name System See **DNS**.

encryption The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications. See also **decryption**.

Ethernet A common local area networking technology in which data is transmitted in units called packets using protocols such as TCP/IP.

Ethernet ID See **MAC address**.

firewall Software that protects the network applications running on your server. IP firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

full name See **long name**.

GB Gigabyte. 1,073,741,824 (2^{30}) bytes.

gigabyte See **GB**.

hacker An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

host Another name for a server.

host name A unique name for a server, historically referred to as the UNIX hostname. The Mac OS X Server host name is used primarily for client access to NFS home directories. A server determines its host name by using the first name available from the following sources: the name specified in the /etc/hostconfig file (HOSTNAME=some-host-name); the name provided by the DHCP or BootP server for the primary IP address; the first name returned by a reverse DNS (address-to-name) query for the primary IP address; the multicast DNS *local hostname*; the name "localhost."

identity certificate See **certificate**.

IMAP Internet Message Access Protocol. A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local computer. Mail remains on the server until the user deletes it.

Internet Generally speaking, a set of interconnected computer networks communicating through a common protocol (TCP/IP). The Internet (note the capitalization) is the most extensive publicly accessible system of interconnected computer networks in the world.

Internet Message Access Protocol See **IMAP**.

Internet Protocol See **IP**.

Internet service provicer See **ISP**.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP address A unique numeric address that identifies a computer on the Internet.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

IPv4 See **IP**.

IPv6 Internet Protocol version 6. The next-generation communication protocol to replace IP (also known as IPv4). IPv6 allows a greater number of network addresses and can reduce routing loads across the Internet.

ISP Internet service provider. A business that sells Internet access and often provides web hosting for ecommerce applications as well as mail services.

KB Kilobyte. 1,024 (2^{10}) bytes.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

kilobyte See **KB**.

LDA Local delivery agent. A mail service agent that transfers mail messages from incoming mail storage to the email recipient's inbox. The LDA is responsible for handling local delivery of messages and for making mail accessible to the user's email application.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

Lightweight Directory Access Protocol See **LDAP**.

list administrator A mailing list administrator. List administrators can add or remove subscribers from a mailing list and designate other list administrators. List administrators aren't necessarily local machine or domain administrators.

local domain A directory domain that can be accessed only by the computer on which it resides.

local hostname A name that designates a computer on a local subnet. It can be used without a global DNS system to resolve names to IP addresses. It consists of lower case letters, numbers, or hyphens (except as the last characters), and ends with ".local" (e.g, bills-computer.local). Although the name is derived by default from the computer name, a user can specify this name in the Network pane of System Preferences. It can be changed easily, and can be used anywhere a DNS name or fully qualified domain name is used. It can only resolve on the same subnet as the computer using it.

long name The long form of a user or group name. See also **user name**.

MAA Mail access agent. A mail service that communicates with a user's email program to download mail message headers to the user's local computer.

MAC address Media access control address. A hardware address that uniquely identifies each node on a network. For AirPort devices, the MAC address is called the AirPort ID.

Mac OS X The latest version of the Apple operating system. Mac OS X combines the reliability of UNIX with the ease of use of Macintosh.

Mac OS X Server An industrial-strength server platform that supports Mac, Windows, UNIX, and Linux clients out of the box and provides a suite of scalable workgroup and network services plus advanced remote management tools.

mail access agent See **MAA**.

mail exchange record See **MX record**.

mail host The computer that provides your mail service.

mail transfer agent See **MTA**.

mail user agent See **MUA**.

mailing list A mail service used to distribute a single email message to multiple recipients. Mailing list subscribers do not have to be mail users on your mail server. Mailing lists can be administered by someone other than a workgroup or server administrator. Mailing list subscribers can often add or remove themselves from lists.

MB Megabyte. 1,048,576 (2^{20}) bytes.

megabyte See **MB**.

MTA Mail Transfer Agent. A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

MUA Mail user agent. A mail process on a user's local computer that works with the MAA to download mail messages and headers to the user's local computer. This is most commonly referred to as an email application, or email program.

MX record Mail exchange record. An entry in a DNS table that specifies which computer manages mail for an Internet domain. When a mail server has mail to deliver to an Internet domain, the mail server requests the MX record for the domain. The server sends the mail to the computer specified in the MX record.

name server A server on a network that keeps a list of names and the IP addresses associated with each name. See also **DNS**.

node A processing location. A node can be a computer or some other device, such as a printer. Each node has a unique network address. In Xsan, a node is any computer connected to a storage area network.

open relay A server that receives and automatically forwards mail to another server. Junk mail senders exploit open relay servers to avoid having their own mail servers blacklisted as sources of junk mail.

Open Relay Behavior-modification System See **ORBS**.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

ORBS Open Relay Behavior-modification System. An Internet service that blacklists mail servers known to be or suspected of being open relays for senders of junk mail. ORBS servers are also known as "black-hole" servers.

permissions Settings that define the kind of access users have to shared items in a file system. You can assign four types of permissions to a share point, folder, or file: read/write, read-only, write-only, and none (no access). See also **privileges**.

plaintext Text that hasn't been encrypted.

POP Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

port A sort of virtual mail slot. A server uses port numbers to determine which application should receive data packets. Firewalls use port numbers to determine whether or not data packets are allowed to traverse a local network. "Port" usually refers to either a TCP or UDP port.

Post Office Protocol See **POP**.

private key One of two asymmetric keys used in a PKI security system. The private key is not distributed and usually encrypted with a passphrase by the owner. It can digitally sign a message or certificate, claiming authenticity. It can decrypt messages encrypted with the corresponding public key. Finally, it can encrypt messages that can only be decrypted by the private key.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

public key One of two asymmetric keys used in a PKI security system. The public key is distributed to other communicating parties. It can encrypt messages that can be decrypted only by the holder of the corresponding private key, and it can verify the signature on a message originating from a corresponding private key.

public key certificate See **certificate**.

public key cryptography A method of encrypting data that uses a pair of keys, one public and the other private, that are obtained from a certification authority. One key is used to encrypt messages, and the other key to decrypt them.

public key infrastructure A secure method of exchanging data over an unsecure public network, such as the Internet, by using public key cryptography.

queue An orderly waiting area where items wait for some type of attention from the system.

RBL Real-time black-hole list. An Internet service that blacklists mail servers known to be or suspected of being open relays for senders of junk mail.

real-time black-hole list See **RBL**.

record type A specific category of records, such as users, computers, and mounts. For each record type, a directory domain may contain any number of records.

relay In QuickTime Streaming Server, a relay receives an incoming stream and then forwards that stream to one or more streaming servers. Relays can reduce Internet bandwidth consumption and are useful for broadcasts with numerous viewers in different locations. In Internet mail terms, a relay is a mail SMTP server that sends incoming mail to another SMTP server, but not to its final destination.

relay point See **open relay**.

round robin An Xsan storage pool allocation strategy. In a volume consisting of more than one storage pool, Xsan allocates space for successive writes to each available pool in turn.

Secure Sockets Layer See **SSL**.

short name An abbreviated name for a user. The short name is used by Mac OS X for home directories, authentication, and email addresses.

Simple Mail Transfer Protocol See **SMTP**.

SMTP Simple Mail Transfer Protocol. A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

spam Unsolicited email; junk mail.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

static IP address An IP address that's assigned to a computer or device once and is never changed.

subdomain Sometimes called the host name. Part of the domain name of a computer on the Internet. It does not include the domain or the top-level domain (TLD) designator (for example, .com, .net, .us, .uk). The domain name "www.example.com" consists of the subdomain "www," the domain "example," and the top level domain "com."

TB Terabyte. 1,099,511,627,776 (2^{40}) bytes.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

terabyte See **TB**.

UCE Unsolicited commercial email. See **spam**.

UDP User Datagram Protocol. A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

user name The long name for a user, sometimes referred to as the user's "real" name. See also **short name**.

virtual domain Another domain that can be used in email addresses for your mail users. Also, a list of all the domain names for which your mail server is responsible.

virtual user An alternate email address (short name) for a user. Similar to an alias, but it involves creating another user account.

WAN Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

wide area network See **WAN**.

wildcard A range of possible values for any segment of an IP address.

Index

A

access
- ACLs 33
- administrator 62
- anonymous 29, 44
- connection control 43, 45, 46
- frequency of user 65
- *See also* IMAP

ACLs (access control lists) 33
addresses. *See* email addresses
administrator
- account for 35
- folder access 62
- mailing list 73, 79, 80

aliases
- local host 37
- user email 23, 35, 38

anonymous user access 29, 44
APOP (authenticated POP) 26
archiving 63, 66, 82
authenticated POP. *See* APOP
authentication
- IMAP 27
- Kerberos 26, 27, 30
- plain text 31
- POP 26
- SMTP 29, 31, 44, 45

B

backups, mail 61
bayesian filters 47
Bcc (blind carbon copies), mail messages 63
blacklisted servers 43, 45
bounced message options 77

C

Certificate Authority (CA) 20
certificates 20, 27
Certificate Signing Request. *See* CSR
ClamAV 47, 50
clear text passwords 26
clients
- mail configuration 34
- and SSL 19
- *See also* users

command line tools
- Cyrus 51
- ditto 61
- and Postfix email aliases 36
- sudo 54

configuration
- clients 34
- incoming mail 24, 25, 26, 27, 29
- outgoing mail 29, 31, 32
- overview 13, 21, 24
- WebMail 17
- *See also* Mailman setup

CRAM-MD5 authentication 27, 30
cyradm tool 51
Cyrus mail service 14, 16, 51, 67

D

database, mail 57, 58, 59, 60
disks
- full disk errors 67
- mail quotas 41, 42
- reclaiming space from logs 67

ditto tool 61
DNS (Domain Name System) service 18
documentation 9, 10, 11
Domain Name System. *See* DNS

E

email. *See* mail service
email addresses 35
email client software 34
encryption 26

F

file systems, mail storage limits 17
filters
- blacklisted mail senders 43, 45
- junk mail 47, 49
- virus 43, 50

firewall, sending mail through 46

forwarding mail 37, 52, 67

G

groups, blind carbon copies 63
groups-based mailing lists 72

H

help, using 8
hosts. *See* servers

I

IMAP (Internet Message Access Protocol)
  administrator access 62
  authentication 27
  cyradm tool 51
  enabling 25
  log 65
  mail quotas 41
  overview 14, 15
  and WebMail 17
incoming mail
  blocking 56
  mail location 16
  message size limits 32
  overview 14
  protocol settings 57
  security 19
  setup 24, 25, 26, 27, 29
  Sieve scripting support 51, 52, 53
  undeliverable 67
information page, mailing list 80
Internet Message Access Protocol. *See* IMAP
Internet service provider. *See* ISP
IP addresses 18, 45
ISP (Internet service provider) 18

J

junk mail screening
  connection control 43, 45, 46
  filters 47, 49
  log 65
  open relay dangers 29
  overview 43
  Sieve scripting 53

K

Kerberos 26, 27, 30

L

list manager 80
local delivery directory 25
logs 65, 66, 67

M

Mac OS X Server, email aliases 35
mail exchange. *See* MX
mailing lists
  administration of 79, 80, 81
  groups-based 72
  overview 71
  viewing 80
  See also Mailman setup; subscribers
Mailman setup
  adding subscribers 78
  bounced message options 77
  creating mailing list 74
  description 75
  enabling 73
  maximum message length 75
  moderator 77, 81
  naming list 74
  overview 72
  privacy option 78
  unsubscribe message 76
  welcome message 76
mail message, subscribing to lists by 84, 85
mail servers, clustering 62
mail service
  backup and restoration 61
  client configuration 34
  improving performance 57
  logs 65, 66
  mail database 57, 58, 59, 60
  mail store 57, 58, 59, 60
  monitoring of 62, 63, 64, 65, 66, 67
  and network services 18
  protocols for 14, 15
  quota management 41, 42
  reloading 56
  resources 69
  saving messages 63
  security 19, 20
  settings 21
  setup overview 21, 23
  starting 23, 55
  stopping 55, 61
  storage of mail 16, 17, 57, 58, 59, 60
  undeliverable mail 67, 68
  upgrading 21
  WebMail 17
  See also incoming mail; mailing lists; outgoing mail
mail store 57, 58, 59, 60
mail transfer agent. *See* MTA
maximum message length 75
messages. *See* mail service
migration, mail service 59
MIME (Multipurpose Internet Mail Extensions) 54, 88
moderator, mailing list 77, 81
MTA (mail transfer agent) 14
Multipurpose Internet Mail Extensions. *See* MIME

MX (mail exchange) 18, 22

N

network services 18

O

open relay 29
outgoing mail
  clearing messages from queue 65
  holding 56
  mail location 16
  protocol overview 14
  queue checking 64
  security 19
  setup 29, 31, 32
  undelivered 68

P

passwords 26, 27, 73, 86
plain text authentication 31
plain text for mailing list messages 88
POP (Post Office Protocol) 14, 15, 24, 25, 27, 65
Postfix transfer agent 14, 36, 67
postmaster alias 23
Post Office Protocol. *See* POP
privacy option, mailing list 78
protocols
  overview 14, 15
  POP 14, 15, 24, 25, 27, 65
  settings 57
  See also IMAP; SMTP

Q

quotas, mail 41, 42

R

relay server, mail 29

S

screening. *See* junk mail screening; virus screening
Secure Sockets Layer. *See* SSL
security
  firewall 46
  overview 19
  passwords 26, 27, 73, 86
  SSL 19, 27, 28, 31
self-signed certificates 20
Sendmail transfer agent 14
Server Admin 22, 33, 55, 64, 80
server administrator 35
servers
  blacklisted 43, 45
  clustering of 62
  hosted virtual domains 37
  IMAP 15
  mail demands on 57
  POP 15
  relay 29
  SMTP 32, 44
  virtual hosting 37
short name 38
Sieve scripting 51, 52, 53
SMTP (Simple Mail Transfer Protocol)
  authentication 29, 31, 44, 45
  connection control 44, 46
  enabling 29
  and holding mail 46
  junk mail screening 44, 45
  log 65
  overview 14
  relay through intermediate server 32
  restricting relay 44, 45
  and WebMail 17
spam. *See* junk mail screening
SpamAssassin. *See* junk mail screening
SquirrelMail. *See* WebMail
SSL (Secure Sockets Layer) 19, 27, 28, 31
subscribers, mailing list
  adding 78, 82
  creating mailing list 74
  digest mode 87, 88
  disabling list delivery 87
  password changes 86
  posting privileges 83
  removing 83
  subscribing options 84
  suspending 84
  unsubscribing options 76, 85
sudo tool 54

T

timsieved process 51

U

UCE (unsolicited commercial email). *See* junk mail screening
undeliverable mail 67, 68
unsolicited mail. *See* junk mail screening
unsubscribing, mailing list 76, 85
upgrading
  mail store and database 59
  to Mac OS X Server 21
user accounts
  access frequency checking 65
  administrator 35
  email aliases 23, 35, 38
  settings' effect on service 21
  setup 34
username 74
users

blind carbon copies 63
database repair for 58
disk quotas 41, 42
forwarding mail 37
and mail service 18
mail user agent 16
and server demand 57
Sieve scripting support 51, 52, 53
subscriber options for mailing lists 84, 85, 88
undeliverable mail 67, 68
viewing list of 64
and virtual hosting 37

V

vacation notification script 52
virtual hosting 37
virus screening 43, 47, 50, 65
volumes, mail storage limits 17

W

web-based interface, mailing lists 80, 81, 84, 85, 86
WebMail 17
web services, mail considerations 17
welcome message, mailing list 76
Workgroup Manager 33, 34
workgroups vs. mailing lists 71

X

Xsan, clustering mail server 62