

Mac OS X Server Administrator's Guide

Includes information on how Mac OS X Server software works
and strategies for using it with your network



Apple Computer, Inc.

© 2001 Apple Computer, Inc. All rights reserved.

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of Apple.

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AppleScript, AppleShare, AppleTalk, ColorSync, Final Cut Pro, FireWire, Keychain, Mac, Macintosh, Power Macintosh, QuickTime, Sherlock, and WebObjects are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. AirPort, Extensions Manager, Finder, iMac, iMovie, and Power Mac are trademarks of Apple Computer, Inc.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Netscape Navigator is a trademark of Netscape Communications Corporation.

RealAudio is a trademark of Progressive Networks, Inc.

© 1995-2001 The Apache Group. All rights reserved.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

062-8441/7-26-01



Contents

Preface

How to Use This Guide 15

- What's Included in This Guide 15
- Setting Up Mac OS X Server for the First Time 16
- Getting Help for Everyday Management Tasks 16
- Getting Additional Information 17

1 Mac OS X Server Administration 19

- What Is Mac OS X Server? 19
- Using Mac OS X Server 20
 - K–12 Classrooms and Labs 21
 - Higher Education Facilities 22
 - Design and Publishing Businesses 24
 - Web Service Providers 25
- Services Included With Mac OS X Server 26
 - Directory Services 26
 - File Services 26
 - Print Service 27
 - Web Service 27
 - Mail Service 28
 - QuickTime Streaming Service 28
 - Client Management Services 28
 - Network Services 28
 - Application Services 30
- How You Administer the Services 30
 - Server Admin 31

Macintosh Manager	34
Streaming Server Admin	34
NetBoot Desktop Admin	35
Setting Up Your Server for the First Time	35
<i>Step 1:</i> Get acquainted with the server and its administration applications	35
<i>Step 2:</i> Install the server	35
<i>Step 3:</i> Log in	35
<i>Step 4:</i> Create share points	36
<i>Step 5:</i> Define default home directory settings	36
<i>Step 6:</i> Define users	36
<i>Step 7:</i> Define groups	37
<i>Step 8:</i> Assign privileges to share points	38
<i>Step 9:</i> Set up additional services as required	38
Where to Find More Information About Mac OS X Server and Server Management	40
If You're New to Server and Network Management	40
If You're an Experienced Server Administrator	40

2 Directory Services 41

What Are Directory Services?	41
User Information Needed for Authentication	41
Other User Information Needed by the Server	41
Where You Can Define User Information	42
How the Server Finds User Information	45
Using NetInfo	46
Before You Set Up NetInfo	46
Setting Up NetInfo for the First Time	50
Using LDAP	51
Before You Set Up LDAP Server Access	51
Setting Up LDAP for the First Time	51
Setting Up Search Policies	52
Before You Set Up Your Search Policy	55
Setting Up Search Policies for the First Time	55

3 Users and Groups 57

What Are Users and Groups?	57
----------------------------	----

How User Information Is Used	57
Characteristics of Users	58
Characteristics of Groups	59
Before You Set Up Users and Groups	59
Setting Up Users and Groups for the First Time	59
<i>Step 1:</i> Modify the administrator account defined at server setup	59
<i>Step 2:</i> Create new users	60
<i>Step 3:</i> Create new groups (optional)	60
User Settings	60
General User Settings	61
Advanced User Settings	62
User Comment	65
Mail Service Settings	65
Group Settings	68
Users and Groups Strategies and Tips	70
Exporting and Importing Users and Groups	70
Setting Up Home Directories to Mount Automatically	70
Mac OS X Server Password Restrictions	71
Solving Problems With Users and Groups	72

4 Sharing 73

What Is Sharing?	73
Before You Assign Privileges	73
Explicit Privileges	74
Types of Privileges	74
User Categories	74
Client Users and Privileges	75
Security Issues	75
Setting Up Sharing for the First Time	76
<i>Step 1:</i> Turn file service on	77
<i>Step 2:</i> Create a share point	77
<i>Step 3:</i> Set privileges for share points	77
Sharing Settings	78
General Settings	78
Automount Settings	80

NFS Access Control Settings	81
Solving Problems With Sharing	82
5 File Services 83	
What Are File Services?	83
Before You Set Up File Services	83
Setting File and Folder Privileges	83
Restricting Guest Access	84
Allowing Access to Registered Users Only	84
Apple File Service	85
Before You Set Up Apple File Service	85
Setting Up Apple File Service for the First Time	85
Apple File Service Settings	86
Solving Problems With Apple File Service	91
Apple File Service Specifications	92
Windows Services	93
Before You Set Up Windows Services	93
Setting Up Windows Services for the First Time	94
Windows Services Settings	95
Solving Problems With Windows Services	99
Windows Services Specifications	99
Network File System (NFS) Service	100
Who Should Use NFS Service?	100
Before You Set Up NFS Service	100
Setting Up NFS for the First Time	101
NFS Service Settings	101
NFS Access Control Settings	102
File Transfer Protocol (FTP) Service	104
Before You Set Up FTP Service	104
Setting Up FTP Service for the First Time	104
FTP Service Settings	105
FTP Service Strategies and Tips	106
Inside FTP Service	106
Solving Problems With FTP Service	108
FTP Service Specifications	109

6 Print Service 111

What Is Print Service? 111
Connecting Printers to the Server 111
Sharing Queues Over the Network 112
Managing Print Queues and Their Jobs 113
Monitoring Print Jobs 113
Before You Set Up Print Service 113
Setting Up Print Service for the First Time 114
<i>Step 1:</i> Add printers 114
<i>Step 2:</i> Configure print service 114
<i>Step 3:</i> Configure print queues 114
<i>Step 4:</i> Start print service 114
<i>Step 5:</i> Enable Windows services (optional) 114
<i>Step 6:</i> Set up printing from client computers 114
Print Service Settings 115
General Print Service Settings 115
Print Queue Settings 116
Print Job Settings 117
Solving Problems With Print Service 118

7 Web Service 121

What Is Web Service? 121
Before You Set Up Web Service 121
Configuring Web Service 122
Providing Secure Transactions 122
Setting Up Web Sites 122
Hosting More Than One Web Site 122
Understanding WebDAV Security 123
Setting Up Web Service for the First Time 123
<i>Step 1:</i> Set up the Documents folder 123
<i>Step 2:</i> Create a default page 124
<i>Step 3:</i> Assign privileges for your Web site 124
<i>Step 4:</i> Configure Web service 124

<i>Step 5:</i> Start Web service	124
<i>Step 6:</i> Connect to your Web site	124
Web Service Settings	125
General Settings for Web Service	125
Sites Settings for Web Service	127
MIME Types Settings for Web Service	128
Proxy Settings for Web Service	129
Web Site Settings	130
General Settings for Web Sites	131
Logging Settings for Web Sites	133
Access Settings for Web Sites	134
Security Settings for Web Sites	136
Strategies and Tips for Web Service	137
Using Persistent Connections to Improve Server Performance	137
Working With Web Modules	138
Using a Common Gateway Interface (CGI) Script	140
Understanding Multipurpose Internet Mail Extension (MIME)	141
Setting Up Secure Sockets Layer (SSL) Service	142
Monitoring Service Activity and Performance	146
Advanced Apache Configuration	147
Disabling the Cache for Dynamic Web Pages	148
Understanding WebDAV Realms and Privileges	149
Solving Problems With Web Service	149
Web Service Specifications	150
Where to Find More Information About Web Service	151

8 Mail Service 153

What Is Mail Service?	153
Post Office Protocol	153
Internet Message Access Protocol	154
Simple Mail Transfer Protocol	154
Before You Set Up Mail Service	154
Mail Service for a Single Server	154
Mail Service for Multiple Domains	154
MX Records for Internet-Based Mail Service	155

Setting Up Mail Service for the First Time	155
<i>Step 1:</i> Set up MX records	155
<i>Step 2:</i> Start mail service	155
<i>Step 3:</i> Configure mail service	156
<i>Step 4:</i> Select default host settings	157
<i>Step 5:</i> Enable mail for users and create a postmaster account	157
Mail Service Settings	158
General Settings	158
Messages Settings	159
Filter Settings	160
Protocols Settings	162
Host Settings	166
Incoming Mail Settings	166
Outgoing Mail Settings	167
Network Settings	169
Where to Find More Information About Mail Service	170

9 QuickTime Streaming Server 173

What Is QuickTime Streaming Server?	173
Viewing Streamed Media: How It Works	173
Who Should Use QuickTime Streaming Server?	174
Before You Set Up QuickTime Streaming Server	174
Sample Setup for Live Video	175
Setting Up QuickTime Streaming Server for the First Time	175
<i>Step 1:</i> Open Streaming Server Admin	176
<i>Step 2:</i> Choose your streaming server settings	176
<i>Step 3:</i> Set up a Web page to show streamed media (optional)	176
Streaming Server Settings	177
General Settings	177
Logging Settings	178
Connected Users	179
Streaming Server Strategies and Tips	179
Preparing Live Media for Streaming	179
Preparing Stored Media for Streaming	180
Using Playlists to Broadcast Prerecorded Audio or Video	181

Inside QuickTime Streaming Server	184
Compatible File Formats	184
Controlling Access to Streamed Media	185
Getting Media Through Firewalls or Networks With Address Translation	188
Setting Up a Relay	189
Solving Problems With QuickTime Streaming Server	192
Where to Find More Information About QuickTime Streaming Server	194

10 Macintosh Management Service 195

What Is Macintosh Management Service?	195
Who Should Use Macintosh Management Service?	195
Before You Set Up Macintosh Manager	196
Setting Up Macintosh Manager for the First Time	196
<i>Step 1:</i> Make sure users with home directories exist in Users & Groups	196
<i>Step 2:</i> Make sure Macintosh Management service is running	196
<i>Step 3:</i> Log in as an administrator	196
<i>Step 4:</i> Add user accounts	197
<i>Step 5:</i> Create a Macintosh Manager administrator	197
<i>Step 6:</i> Create a workgroup	197
<i>Step 7:</i> Set security options	197
Macintosh Manager Settings	198
Basic Settings for Users	198
Advanced Settings for Users	200
Members Settings for Workgroups	203
Items Settings for Workgroups	205
Privileges Settings for Workgroups	207
Volumes Settings for Workgroups	211
Printers Settings for Workgroups	213
Options Settings for Workgroups	215
Lists Settings for Computers	217
Workgroups Settings for Computers	218
Control Settings for Computers	219
Security Settings for Computers	221
Log-In Settings for Computers	223
Check Out Settings for Computers	224

Global Security Settings	225
Global CD-ROMs Settings	227
Macintosh Manager Strategies and Tips	228
Providing Quick Access to Unimported Users	228
Setting Up Macintosh Manager on Large or Growing Networks	229
Creating Workgroups to Meet Your Network's Needs	229
Choosing Desktop Environments for Your Workgroups	230
Maximizing Security	231
Inside Macintosh Manager	232
How Macintosh Manager Starts Up	232
How Macintosh Manager Works With Preferences	232
How Macintosh Manager Ensures Security	237
How Client Computers Are Updated From the Server	238
How Macintosh Manager Keeps Track of Users, Workgroups, and Computer Lists	238
About the Macintosh Manager Share Point	239
Using Macintosh Manager and NetBoot Services Together	240
Solving Problems With Macintosh Manager	241
Problems Logging In to Macintosh Manager	241
Problems Client Users May Have	242
Where to Find More Information About Macintosh Manager	243

11 NetBoot 245

What Is NetBoot?	245
Who Should Use NetBoot?	245
Before You Set Up NetBoot	246
Planning Your Network	246
NetBoot Server Worksheet	253
Setting Up NetBoot Server Software for the First Time	254
<i>Step 1:</i> Install NetBoot server software (optional)	254
<i>Step 2:</i> Use the NetBoot Setup Assistant	254
<i>Step 3:</i> Set up Macintosh Manager	255
<i>Step 4:</i> Start up a NetBoot client computer	255
Using NetBoot Desktop Admin	255
Installing Software or Changing the Disk Image	256
NetBoot Strategies and Tips	257

Improving NetBoot Performance	257
Server Performance Factors	258
Inside NetBoot	260
Solving Problems With NetBoot	261
12 Network Services 263	
What Are Network Services?	263
Service Location Protocol (SLP) Directory Agent (DA) Service	264
Who Should Use SLP DA Service?	264
Before You Set Up SLP DA Service	264
Setting Up SLP DA Service for the First Time	265
SLP DA Service Settings	267
SLP DA Service Strategies and Tips	269
Dynamic Host Configuration Protocol (DHCP) Service	271
Who Should Use DHCP Service?	271
Before You Set Up DHCP Service	271
Setting Up DHCP Service for the First Time	272
DHCP Service Settings	274
DHCP Service Strategies and Tips	279
Domain Name System (DNS) Service	280
Who Should Use DNS Service?	280
Before You Set Up DNS Service	280
Setting up DNS Service for the First Time	281
DNS Service Strategies and Tips	282
IP Filter Service	285
What Is IP Filter Service?	285
Who Should Use IP Filter Service?	286
Before You Set Up IP Filter Service	286
Setting Up IP Filter Service for the First Time	289
IP Filter Service Settings	290
IP Filter Window Settings	295
IP Filter Service Strategies and Tips	296
Solving Problems With IP Filter Service	300
Where to Find More Information About Network Services	300

Appendix A Advanced Topics 301

- TCP/IP Topics 301
 - Ports Used by Mac OS X Computers 301
 - Setting Up a Private TCP/IP Network 304
 - Setting Up Multiple IP Addresses for a Port 305
 - Creating IP Filter Rules Using ipfw 306
 - Where to Find More Information About Setting Up TCP/IP 308
- File Format for Importing or Exporting Users and Groups 308
 - Example XML File 308
 - Creating Your Own Users and Groups File 312
 - Where to Find More Information About XML 314
- LDAP Data Specifications 314
 - Mapping User Data 315
 - Mapping Network Service Data 321
 - Using the Default Mappings 322
 - Configuring LDAP Access 323
- Backing Up Server Information 328

Appendix B Mac OS X Server Information Worksheet 329

Glossary 333

Index 339

How to Use This Guide

What's Included in This Guide

Whether you're new to networking or an experienced administrator, this book is your starting point. The chapters you choose to read depend on what you plan to do with your server.

- Read Chapter 1, "Mac OS X Server Administration," for an overview of how Mac OS X Server is used, the services it provides, how you administer it, and how you set it up for the first time.
- Chapters 2, 3, and 4 describe three of the core components of Mac OS X Server—directory services, users and groups, and sharing. Most services depend on how you set up these three components, so it's worthwhile to take the time to read these chapters.
- Chapter 5, "File Services," describes the file services included in Mac OS X Server: Apple file service, Windows services, Network File System (NFS) service, and File Transfer Protocol (FTP) service.
- Chapter 6, "Print Service," tells you how to share PostScript®-compatible printers among users on Macintosh, Windows, and other computers.
- Chapter 7, "Web Service," describes Web service in Mac OS X Server. You'll learn how to set up secure transactions on your Web server and host multiple Web sites.
- Chapter 8, "Mail Service," includes information about mail service in Mac OS X Server, including using mail over the Internet and choosing the best protocols for your network.
- Chapter 9, "QuickTime Streaming Server," describes the service that lets you deliver media over the Internet in real time.
- Chapter 10, "Macintosh Management Service," offers information about how you can use Macintosh Manager to manage your client computers more effectively.
- Chapter 11, "NetBoot," describes NetBoot, which allows administrators to configure and update client computers instantly by simply updating the startup disk image on the server.

- Chapter 12, “Network Services,” presents information about Mac OS X Server’s network services, which include Service Location Protocol (SLP) Directory Agent (DA) service, Dynamic Host Configuration Protocol (DHCP) service, Domain Name System (DNS) service, and IP filter service.
- Appendix A, “Advanced Topics,” provides supplemental information for administrators who want more details about advanced server management.
- Appendix B, “Mac OS X Server Information Worksheet,” provides a form for recording information about your server.
- The glossary lists and defines all the acronyms you’ll encounter as you read this manual.

Read any chapter that’s about a service you plan to provide to your users. Each service’s chapter includes an overview of how the service works, what it can do for you, strategies for using it, and how to set it up for the first time. Also take a look at any chapter that describes a service with which you’re unfamiliar. 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.

Toward the end of some chapters is a section, “Inside” the service, that includes more technical information for the advanced user. You’ll want to read this section if you want a deeper understanding of the software or protocols that are running behind the scenes in a particular service.

Most chapters end with a section called “Where to Find More Information.” This section points you to Web sites and other reference material where you can find more detailed 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. Refer to *Getting Started With Mac OS X Server*, the fold-out card that came with your software, for instructions on server installation and setup. After completing the steps in that document, use the instructions in Chapter 1 of this guide to set up your server for the first time.

Getting Help for Everyday Management Tasks

If you want to change settings, monitor services, view service logs, or do any other management task, you can find step-by-step procedures by using the online help available with each of your server administration programs.

Getting Additional Information

These documents are available at www.apple.com/macosx/server/

- *Mac OS X Server Migration Guide* provides instructions for upgrading to Mac OS X Server from AppleShare IP, Macintosh Manager, and Mac OS X Server 1.2.
- *Understanding and Using NetInfo* describes the built-in Mac OS X directory system and provides instructions for configuring NetInfo and Mac OS X Server to increase the power of your Mac OS X network.

Mac OS X Server Administration

This chapter introduces Mac OS X Server and gives an overview of its administration. It also provides several suggestions for helping you get started with your server:

- “Setting Up Your Server for the First Time” on page 35 provides a procedure for getting your server up and running quickly.
- “Where to Find More Information About Mac OS X Server and Server Management” on page 40 lists resources for server and network management information for both novice and experienced server administrators.

What Is Mac OS X Server?

Mac OS X Server is a powerful server platform that delivers a complete range of services to users on the Internet and the local network:

- It lets you connect users to each other, using such services as mail and file sharing.
- It helps you share system resources, such as printers and computers.
- It can host Internet services, such as Web sites and streaming video.
- It lets you customize what is visible to networked users, such as desktop resources and personal files.

This chapter introduces you to the services included with Mac OS X Server and provides a tour of the programs you use to administer them. First you'll read about how the services can be put to use in educational, publishing, and Internet service environments. Then you'll review the capabilities of individual services and get an introduction to the applications that let you administer them. Finally, you'll find instructions for getting the server up and running.

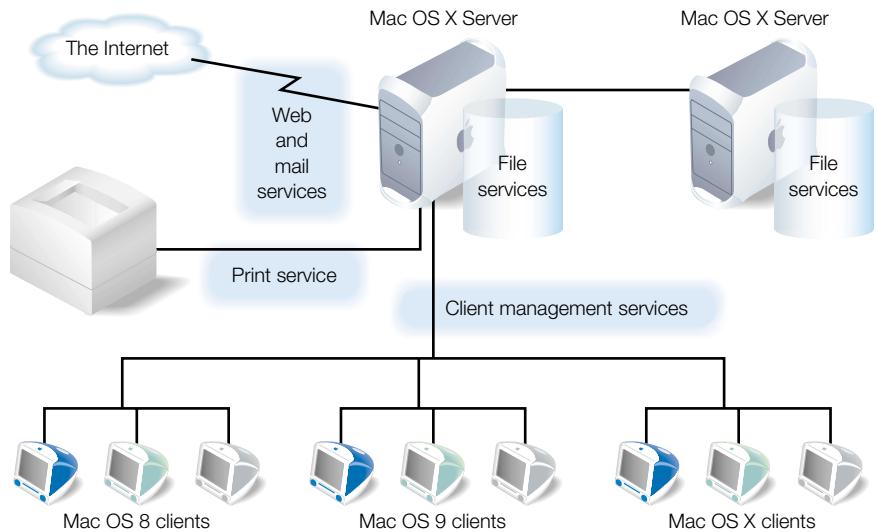
Using Mac OS X Server

Your server can address the needs of many environments. This section gives examples of four common environments:

- K–12 classrooms and labs
- Higher education facilities
- Design and publishing businesses
- Web service providers

K-12 Classrooms and Labs

Servers in any educational environment need to help students access the Internet, send mail, manage files, view videos, and print documents. They also need to help teachers access lesson plans and other classroom materials, as well as student records and centralized administrative information. The Mac OS X Server Web, mail, print, and file services support all these needs:

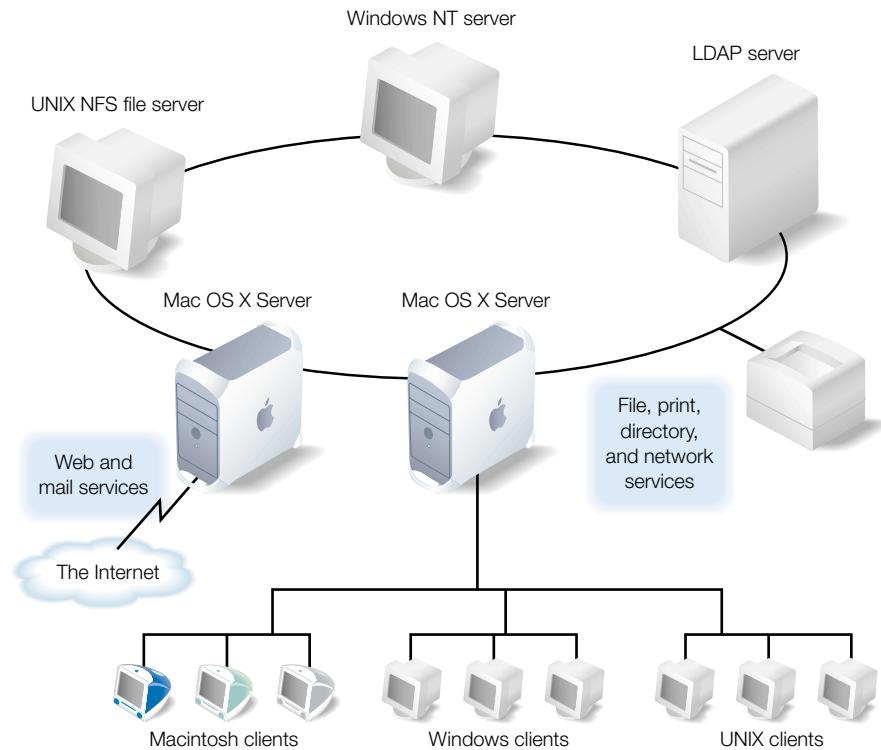


Servers supporting K–12 classrooms and labs have several special requirements:

- They need to provide ways to control the student workstation environment. Mac OS X Server software includes client management services, which let you manage and monitor Macintosh computers used by students.
For example, Macintosh Management service lets you control which applications students can access. You can also define application preferences, desktop patterns, and other personal desktop settings so that students experience the same environment on different computers on the network.
- They must also efficiently handle many simultaneous requests for the same Internet resources. Mac OS X Server provides caching Web proxy service, so that Web content that has already been downloaded doesn't need to be retrieved again from the Internet the next time it is requested.

Higher Education Facilities

In colleges and universities, server requirements are much more complex and varied, because the students and the workstations they use are highly diverse. This complexity requires a complete range of file and network services:

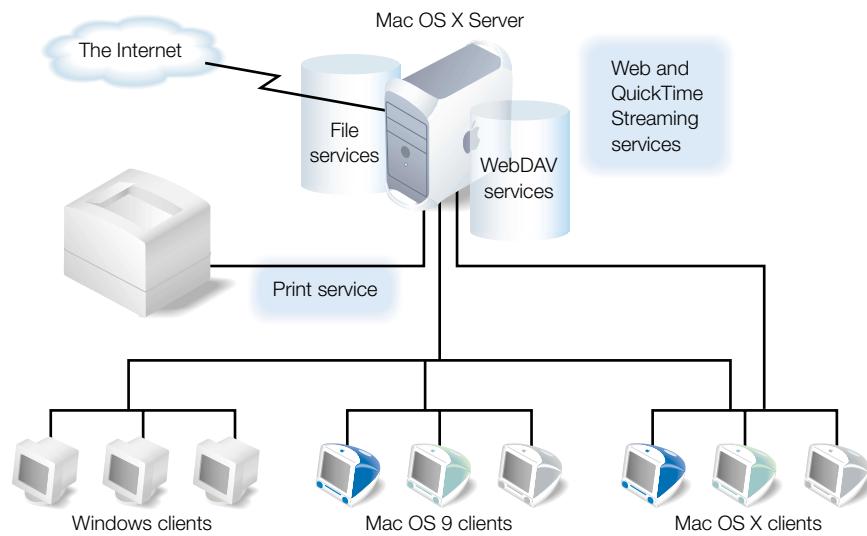


- The wide range of client computers—Macintosh, Windows, UNIX, Linux—demands flexible file access support. The highly scalable IP-based file services in Mac OS X Server support file access from anywhere on the network via Apple Filing Protocol (AFP), Network File System (NFS), File Transfer Protocol (FTP), and Server Message Block (SMB).

- The server offers PostScript-compatible print spooling and job accounting for print jobs submitted using LPR, the industry-standard TCP printing protocol, as well as the Windows SMB protocol.
- Because higher education networks are heterogeneous and complex, network services are critically important. Domain Name System (DNS) and Service Location Protocol (SLP) services are only two examples of services that Mac OS X Server provides to help client computers and services find resources on a network. Dynamic Host Configuration Protocol (DHCP) helps you serve students who log in to the network from portable computers.
- IP filtering, another Mac OS X Server network service, provides a security firewall around sensitive data.
- User and network resource information needs to be retrievable from directory systems, such as NetInfo, and integrated into existing infrastructures, such as Lightweight Directory Access Protocol (LDAP) servers. Mac OS X Server can be easily configured to access this information.

Design and Publishing Businesses

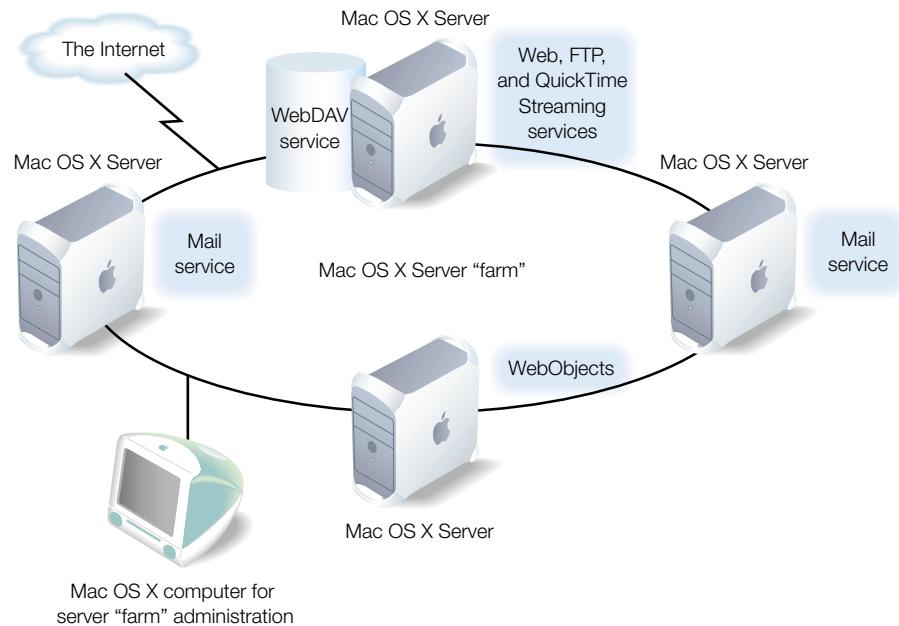
Mac OS X Server provides services that fully support the workflow needs of Internet designers and publishers:



- The popular Apache Web server is built into Mac OS X Server.
- The Web-based Distributed Authoring and Versioning (or WebDAV) technology, integrated into the server's Web service, lets you do drag-and-drop publishing and file sharing from Mac OS X computers.
- For video, QuickTime Streaming service lets you broadcast streaming video to client computers in real time.
- Apple Filing Protocol (AFP) lets you transfer large files among workgroup members.

Web Service Providers

Mac OS X Server provides the support necessary for hosting ecommerce Web sites and providing other Internet services that require high availability and scalability:



- Web service is based on Apache, an open source HTTP Web server. You can host many Web sites on a single server, each with its own address (multilink multihoming). You can configure your server to support multiple addresses per Ethernet card (virtual hosting).
- Web service supports Secure Sockets Layer (SSL) protection for secure Internet connections.
- The server includes deployment components of the WebObjects software suite. These application services let you deploy ecommerce applications that can connect to multiple databases and generate HTML and Java™ dynamically.
- Mac OS X Server also includes built-in support for Perl, Java Servlets, JavaServer Pages, and PHP.
- QuickTime Streaming Server lets you broadcast multimedia in real time to viewers using an industry-standard streaming protocol.
- The server automatically restarts when a service or power failure occurs, maximizing service availability.

Services Included With Mac OS X Server

These Mac OS X Server services are highlighted in this section:

- directory services
- file services
- print service
- Web service
- mail service
- QuickTime Streaming service
- client management services
- network services
- application services

Directory Services

Directory services let your server locate information about users and groups (collections of users) that is needed for authentication and authorization. Directory services let you configure your server to find user information stored right on the server or in a location that has been set up to share information among servers.

While you usually store user information using the built-in NetInfo directory system, your server can also retrieve it from standard Lightweight Directory Access Protocol (LDAP) servers. If you store user names in multiple directory systems, the server automatically searches the locations you specify in the order you prefer when it needs to validate a user.

File Services

File services allow your client users to access files, applications, and other resources over a network. Mac OS X Server includes these file services:

- Apple file service
- Windows services
- FTP service
- NFS service

Apple File Service

Apple file service, which uses the Apple Filing Protocol (AFP), lets you share resources with Macintosh clients. Macintosh users can connect to your server and access folders and files as if they were located on their own computers. Mac OS X users access your server using the Connect To Server command in the Finder's Go menu; you can also automatically mount directories on Mac OS X computers when they start up. Mac OS 8 and Mac OS 9 users use the Chooser or Network Browser. Apple file service is fully integrated into the operating system environment, providing support for such features as file aliases and Sherlock.

Windows Services

Windows services let users of Windows or Windows-compatible computers take advantage of Mac OS X Server resources. Without any additional software, Windows users can find your server and browse for files and print queues using their familiar Network Neighborhood windows.

FTP Service

File Transfer Protocol (FTP) lets users transfer files over the Internet. Users of any computer that supports FTP can download files from your server—usually by using an Internet browser or FTP client application. FTP also offers a standard way for both known and anonymous users to transfer files to and from your server.

NFS Service

Network File System (NFS) service lets you make directories (folders) available for users who have NFS client software. NFS is often used to export directories for UNIX clients.

Print Service

Print service lets you share PostScript-compatible printers among users who submit print jobs from Macintosh, Windows, and UNIX computers. Any user whose computer is configured to print using the standard LPR protocol or the Windows SMB protocol can submit print jobs to printers you configure your server to manage.

Web Service

The heart of Mac OS X Server Web service is Apache, the dominant open source Web server. If you are already familiar with Apache, you will continue to enjoy its log file analysis tools, configuration file handling, and readily available documentation.

Web service in Mac OS X Server also offers you the ability to customize your Web environment. You can set up Web sites for as many domains as you'd like, configure secure (SSL-based) communications on a per site basis, and use the built-in support for such application services as CGI, WebObjects, Perl, PHP, and Java Servlets.

Web service includes Web-based Distributed Authoring and Versioning (WebDAV), which lets users check out Web pages, make changes, then check them back in while the site is running. WebDAV essentially provides a file server specifically for Web content authors.

Mail Service

Mail service lets you provide email service for users over your network or over the Internet. The service provides multiple-domain mail support as well as built-in junk mail protection. It supports all the standard mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP).

To provide mail service over the Internet, you can define Domain Name System (DNS) services on your network or use DNS services offered by your Internet service provider (ISP). DNS is one of the Mac OS X Server network services and is required for SMTP mail handling.

QuickTime Streaming Service

QuickTime Streaming Server lets you stream multimedia in real time using the industry-standard RTSP/RTP protocol.

You can deliver live and prerecorded media over the Internet to both Macintosh and Windows users, or relay streamed media to other streaming servers. You can provide unicast streaming, which sends one stream to each individual client, or multicast streaming, which sends the stream to a group of clients.

Client Management Services

Client management services let you simplify and control the environment that Macintosh client users experience.

Macintosh Management Service

Macintosh Management service lets you set network-wide policies for controlling user access to applications, home directories, and printers. You can also define the environment users see when they log in. You can use this service to manage clients with Mac OS 8.1 or later installed.

NetBoot

NetBoot allows Macintosh client computers to start up using a Mac OS 9 operating system provided by a Mac OS X Server.

NetBoot lets you configure and update Mac OS 9 computers by simply updating their startup image. The server hosts a startup image that contains a System Folder and applications folder for all Mac OS 9 computers. Any changes made on the server are automatically reflected on the client computers when they restart.

Network Services

Mac OS X Server includes these network services for helping you manage Internet communications on your TCP/IP network:

- SLP DA service

- DHCP service
- DNS service
- IP filter service

SLP DA Service

Service Location Protocol (SLP) provides structure to the services available on a network and gives users easy access to them.

Anything that can be addressed using a URL can be a network service—for example, file servers and WebDAV servers. When a service is added to your network, it uses SLP to register itself on the network; you don't need to configure it manually. When a client computer needs to locate a network service, it uses SLP to look for services of that type. All registered services that match the client computer's request are displayed for the user, who then can choose which one to use.

SLP Directory Agent (DA) is an improvement on basic SLP, providing a centralized repository for registered network services. You can set up a DA to keep track of services for one or more *scopes* (groups of services). When a client computer looks for network services, the DA for the scope in which the client computer is connected responds with a list of available network services. Because a client computer only needs to look locally for services, network traffic is kept to a minimum and users can connect to network services more quickly.

DHCP Service

Dynamic Host Configuration Protocol (DHCP) is a protocol that helps you administer and distribute IP addresses dynamically to client computers from your server. From a block of IP addresses that you define, your server locates an unused address and “leases” it to client computers as needed. DHCP is especially useful when an organization has more clients than IP addresses. IP addresses are assigned on an as-needed basis, and when they are not needed, they are available for use by other clients.

DNS Service

Domain Name System (DNS) service lets users connect to a network resource, such as a Web or file server, by specifying a domain name (such as `server.apple.com`) rather than an IP address (`192.168.11.12`). DNS is a distributed database that maps IP addresses to domain names.

A server that provides DNS service keeps a list of names and the IP addresses associated with the names. When a computer needs to find the IP address for a name, it sends a message to the DNS server (also known as a *name server*). The name server looks up the IP address and sends it back to the computer. If the name server doesn't have the IP address locally, it sends messages to other name servers on the Internet until the IP address is found.

You will use DNS if you use SMTP mail service or if you want to create subdomains within your primary domain. You will also use DNS if you are hosting multiple Web sites. If you don't have an ISP who handles DNS for your network, you can set up a DNS server on your Mac OS X Server.

IP Filter Service

IP filter service protects your server and the content you store on it from intruders. It provides a software firewall, scanning incoming IP packets and accepting or rejecting them based on filters you define.

You can set up server-wide restrictions for packets from specific IP addresses. You can also restrict access to individual services—such as Web, mail, and FTP—by defining filters for the ports used by the services.

Application Services

WebObjects offers a flexible and scalable way to develop and deploy ecommerce and other Internet applications. WebObjects applications can connect to multiple databases and dynamically generate HTML content.

Your server includes the WebObjects deployment system and an unlimited license to deploy your WebObjects applications. You can also purchase the WebObjects development tools if you want to create WebObjects applications.

The remainder of this guide does not address WebObjects. For more information and documentation on WebObjects, go to the WebObjects Web page:

www.apple.com

How You Administer the Services

This section introduces the administration applications you use to configure and manage the services in Mac OS X Server and tells you how to get started using them:

- *Server Admin*: You use Server Admin to configure and manage most services, to set up and manage server user accounts, and to configure share points (items such as folders and disks you want users to share on the server).

You can use Server Admin either on your server or remotely, using secure, encrypted communications between a computer running Mac OS X or another server and the server you are administering. Server Admin has an individual module for managing each service. See “Server Admin” on page 31 for more information.

- *Macintosh Manager*: Use Macintosh Manager to set up authentication and define user environments for computers with Mac OS 8.1 through Mac OS 9.1 installed.

This application, described in “Macintosh Manager” on page 34, can be used on computers with Mac OS 9 or later installed.

- *Streaming Server Admin:* This browser-based application lets you set up and manage streaming service from a Web browser.
You can use this application, described in “Streaming Server Admin” on page 34, from any computer that has Netscape Navigator™, Netscape Communicator, or Microsoft Internet Explorer, versions 4.5 or later, installed.
- *NetBoot Desktop Admin:* Use NetBoot Desktop Admin to install, update, or remove items from the system image your NetBoot clients use to start up.
You can use NetBoot Desktop Admin from a client computer with Mac OS 9 installed. See “NetBoot Desktop Admin” on page 35 for more information about this application.

Server Admin

You can use Server Admin locally (at the server) or remotely (from a computer running Mac OS X or another Mac OS X Server) to administer services on one or more Mac OS X Servers.

When you install Mac OS X Server, Server Admin is automatically installed on the server. To install the remote Server Admin component on a computer running Mac OS X, follow these steps:

- 1 On a Mac OS X computer with networking configured, insert the Mac OS X Server CD.
- 2 Open the Admin Install folder and double-click the installer package, Admin_Install.mpkg.
- 3 Choose the Custom Install option, then select Server Admin.

Server Admin is installed in /Applications/Utilities/.

Logging in to Server Admin

To log in to Server Admin:

- 1 Open Server Admin (located in /Applications/Utilities/) by clicking the Server Admin icon in the Dock:



- 2 Enter the IP address or domain name of the Mac OS X Server you want to administer. By default, the IP address of the local server appears in the login window. To administer a different server, enter that server’s address or domain name. Then enter the administrator’s user name and password for the server.
- 3 Click Connect.

You can manage multiple servers simultaneously by logging in to each server and administering it from its own toolbar.

Getting Acquainted With the Toolbar

After you open Server Admin and log in to a server, a toolbar for that server appears. You administer services by using the service modules, which are arranged on four tabs in the toolbar.



Here is a summary of when to use the service modules and where to find more information about them in this guide:

To do this	Use this module	Go here for more info
View information about your server	Server Info module (in the General tab)	page 34
View server logs	Log Viewer (in the General tab)	page 33
Set up and manage directory services	Mac OS X utilities for Directory Services	page 41
Set up and manage users	Users & Groups module (in the General tab) Sharing module (in the General tab)	page 57 page 73
Work with Macintosh Management service	Macintosh Mgr module (in the General tab)	page 195
Set up and manage file services	Modules in the File & Print tab: <ul style="list-style-type: none">■ Apple file service■ Windows services■ FTP service■ NFS service	page 85 page 93 page 104 page 100
Set up and manage print service	Print module (in the File & Print tab)	page 111

To do this	Use this module	Go here for more info
Set up and manage Web service	Web module (In the Internet tab)	page 121
Set up and manage mail service	Mail module (in the Internet tab)	page 153
Set up and manage network services	Modules in the Network tab	
■ SLP DA service	■ SLP Service	page 264
■ DHCP service	■ DHCP/NetBoot	page 271
■ DNS service	■ DNS Service	page 280
■ IP filter service	■ IP Filter	page 285

When you click a Server Admin module, a menu of commands appears. For information about how to use the commands to manage your services, refer to the pages indicated in the table above or see the onscreen help for the module. For information about how to use Server Admin in general, look in the Help menu in the Server Admin menu bar.

At the bottom of the toolbar, a status bar indicates how many services are running and alerts you to conditions that warrant your attention. A globe identifies running services, and a triangle containing “!” identifies alerts. These symbols also appear on individual module icons, and on any tab containing a module with an alert.



Viewing Logs

The Log Viewer lets you monitor errors and other noteworthy events logged by various services and applications running on your server. Log Viewer windows are dynamically updated as new log records are written, letting you monitor multiple services in real time.

Click Log Viewer, then choose the service whose logs you want to view. Choose Print Service, for example, to view logs for print service and for each of the server’s print queues. If you don’t see the service you are interested in, make sure the service is running, then check the system log (choose System Software from the Log Viewer menu, then choose System Log from the Display pop-up menu).

Later chapters in this guide and the onscreen help provide information about the logs for particular services. Also refer to the onscreen help for information about using the Log Viewer and setting up and viewing logs maintained by various services.

Getting Information About Your Server

Click Server Info, then choose Show Server Info to view the serial number and networking characteristics of your server.

If you need to change the server's serial number, click Server Info, then choose Change Product Serial Number.

Macintosh Manager

You use the Macintosh Manager application to administer Macintosh Management service and set up user environments for client computers on your network. You can use Macintosh Manager locally (at the server) or remotely (from a Mac OS 9 or Mac OS X computer on the same network as your Mac OS X Server).

In addition to Macintosh Manager, you'll also use two Server Admin modules to administer Macintosh Management service: Users & Groups and Sharing. Details about all these applications can be found starting on page 195.

Logging in to Macintosh Manager

Open Macintosh Manager by clicking its icon in the Dock. Log in using a server administrator user name and password. As a server administrator, you automatically have global administrator privileges for Macintosh Manager. Once you are logged in, you can add users, create workgroups, and manage computers on the network.

You can also open Macintosh Manager by clicking Macintosh Mgr in the Server Admin General tab, then choosing Open Macintosh Manager.

Starting and Stopping Macintosh Management Service

To start and stop Macintosh Management service, use the Macintosh Mgr module of Server Admin. You can also use the Macintosh Mgr module to set whether Macintosh Management service automatically starts when the server starts up.

Streaming Server Admin

You can use Streaming Server Admin from any computer that has a Web browser installed and running. To open Streaming Server Admin, open a browser and enter the URL for Streaming Server Admin on your server. Then enter the streaming server administrator login ID and password. The connection established is secure.

For further information about Streaming Server Admin, see Chapter 9, “QuickTime Streaming Server,” on page 173.

NetBoot Desktop Admin

On a Mac OS 9 computer, use the Chooser to locate the NetBoot server volume, then log in to it as a server administrator. You can then open NetBoot Desktop Admin and make changes to the startup image. Follow the onscreen instructions when using NetBoot Desktop Admin.

You can read more about NetBoot administration starting on page 245.

Setting Up Your Server for the First Time

Follow these steps to get your server up and running quickly. After you complete step 8, users will be able to access the server and take advantage of basic Apple file service features. Step 9 refers you to other places in this guide where you can get instructions for setting up additional services you want to provide your users.

Step 1: Get acquainted with the server and its administration applications

If you haven't already done so, read the earlier sections of this chapter. These sections describe some common scenarios in which Mac OS X Server can be used, in both business and education environments. Then they introduce the services you can provide to your users and survey the applications you use to administer the server.

These sections introduce terms and concepts you'll encounter as you proceed through the remaining steps.

Step 2: Install the server

Use the worksheet and instructions in *Getting Started With Mac OS X Server* to install your server and make it ready to use on your network.

Step 3: Log in

Using the owner/administrator name and password you specified during step 2, log in to the server. Then log in to the Server Admin application:

- 1 Open Server Admin from the Dock or from Applications/Utilities.
- 2 In the Address box, enter the IP address or domain name you assigned to the server during step 2.
- 3 In the User Name box, enter the owner/administrator name. In the Password box, enter the owner/administrator password.
- 4 Click Connect.

Step 4: Create share points

A share point is a hard disk (or hard disk partition), CD-ROM disc, or folder that contains files you want users to share. If you are a teacher, for example, you may want to set up a share point for individual classes—Math, English, Biology—so that students in each class can access their assignments and handouts.

To create share points:

- 1** In a Finder window, open the folder in which you want to create the share point. Choose New Folder from the File menu. Name the share point.
- 2** In Server Admin, click the File & Print tab and make sure that Apple file service is running. If it's not, click Apple and choose Start Apple File Service.
- 3** Click the General tab. Then click Sharing and choose Set Sharing Attributes. Select the folder you created and click Choose.
- 4** Click “Share this item and its contents,” then click Save.
- 5** Repeat steps 1 through 4 for each share point you want to create.

Step 5: Define default home directory settings

A home directory is a folder for a user’s personal files. Each student, for example, might use a home directory for storing class notes or assignments they’re working on.

If you define default home directory settings, a home directory is automatically created for each new user you define on your server. To define default home directory settings:

- 1** In the General tab of Server Admin, click Users & Groups and choose Home Directory Defaults.
- 2** Choose Local to set up a simple default strategy. You can always change your strategy later if you need to.
- 3** Choose the share point in which you want the home directories to reside from the Share Point pop-up list. You can choose the predefined Users share point or one of the share points you created earlier.
- 4** Click Save.

Whenever you define a new user, a home directory will be created for the user in the share point you selected and named using the “short name” you enter for the user. The user owns the home directory, meaning the user has Read & Write access to the directory and has complete control over access to the files in the home directory.

Step 6: Define users

To define the users you want to be able to use your server:

- 1** In the General tab of Server Admin, click Users & Groups and choose New User.

- 2** In the Name field, enter a name that identifies the user (for example, Bob W. Brown, Jr.).
 - 3** In the Short Name field, enter a short name for the user. Although the user can log in to the server using the name you specify in step 2, a short name is more convenient. Also, remember that the user's home directory will be named using the short name. The short name is also used in the user's email address if you set up mail service on the server.

Typically the short name is 8 characters or shorter. Use only letters, numbers, the hyphen character (-), or the underscore character (_).
 - 4** In the Password field, enter the password the user should use to log in to the server. Although you define the password initially, the user can change it when logging in to the server or by using the Password pane in System Preferences. Enter a password that won't be easily guessed by unauthorized users.
- The password is case-sensitive and does not appear on the screen as it is entered. Make sure you have not pressed the Caps Lock key before entering the password. Avoid spaces and Option-key combinations.
- 5** Select "User can administer the server" if you want the user to be able to administer the server. When you first set up the server, only the owner/administrator designated during setup can administer it. Server administrators can use all the server management applications and have complete access to all the server's facilities.
 - 6** Select "User can log on" to let the user log in to the server, then click Save.
 - 7** Repeat steps 1 through 6 for each user you want to be able to access the server.

Step 7: Define groups

Groups are collections of users with similar needs. For example, you can add math students to a math class group and give the group access to files in the math group's share point.

Groups simplify the administration of shared resources. Instead of granting access to those resources to each individual who needs them, you can simply add the users to a group, and grant access to the group.

To define a group:

- 1** In the General tab of Server Admin, click Users & Groups and choose New Group.
- 2** Enter a name for the group. Avoid the space character or Option-key characters if you want to be able to send mail to the group.
- 3** To add users to the group, click Open U&G List. Locate the users you want to add, then drag them into the group settings window.
- 4** Click Save.

Step 8: Assign privileges to share points

To assign access privileges for your share points to the users and groups you have defined:

- 1** In the General tab of Server Admin, click Sharing and choose Show Disks & Share Points.
- 2** Double-click a share point.
- 3** In the General tab, click Users & Groups, then choose Open U&G List.
- 4** To change the share point owner, drag a user from the Users & Groups List window to the Owner field in the sharing window. Use the pop-up menu to the right of the Owner field to set access privileges for the owner.
- 5** To assign access privileges to a group, drag a group from the Users & Groups List window to the Group field in the sharing window. Then use the pop-up menu to the right of the Group field to set access privileges for the group. If the group is a math class group, for example, you may want to grant Read Only access so that math students can read information you place within the share point but not change it.
- 6** To assign access privileges to any user who can log in to the server, use the pop-up menu to the right of Everyone.

Step 9: Set up additional services as required

Decide which additional services you want to set up, then refer to the chapters indicated in the following table. Browse through the chapter first to become familiar with what's in it. Then use the instructions for what to do *before* you set up the service and how to set it up *for the first time*. This information, supplemented by detailed procedures available in the onscreen help, will guide you through setting up individual services.

If you want to	Set up	Instructions are in
Assign access privileges to folders and files within a share point	Folders and files, then assign access privileges	Chapter 4, "Sharing," on page 73
Implement additional Apple file service features	Apple file service	Chapter 5, "File Services," on page 85
Provide file and print services for Windows users	Windows services	Chapter 5, "File Services," on page 93
Make folders available for users with NFS client software	NFS service	Chapter 5, "File Services," on page 100
Let users transfer files from the server using FTP	FTP service	Chapter 5, "File Services," on page 104

If you want to	Set up	Instructions are in
Share printers among users	print service	Chapter 6, “Print Service,” on page 111
Set up Web sites or WebDAV support on the server	Web service	Chapter 7, “Web Service,” on page 121
Provide email service for your users	mail service	Chapter 8, “Mail Service,” on page 153
Broadcast multimedia in real time from the server	QuickTime Streaming Service	Chapter 9, “QuickTime Streaming Server,” on page 173
Manage the environment that Mac OS 8.1 and later users experience	Macintosh Management service	Chapter 10, “Macintosh Management Service,” on page 195
Provide identical System and applications folders for all Mac OS 9 client computers	NetBoot	Chapter 11, “NetBoot,” on page 245
Automate registration for network devices accessible using a URL	SLP DA service	Chapter 12, “Network Services,” on page 263
Assign IP addresses dynamically to client computers	DHCP service	Chapter 12, “Network Services,” on page 271
Set up a domain name server	DNS service	Chapter 12, “Network Services,” on page 280
Filter IP packets that the server receives	IP filter service	Chapter 12, “Network Services,” on page 285
Share user information among multiple Mac OS X Servers and/or Mac OS X computers	directory services	Chapter 2, “Directory Services,” on page 41

Where to Find More Information About Mac OS X Server and Server Management

If You're New to Server and Network Management

If you want to learn more about Mac OS X Server, see the Mac OS X Server Web site:

www.apple.com/macosx/server/

Online discussion groups can put you in touch with your peers. Many of the problems you encounter may already have been solved by other server administrators. To find the lists available through Apple, see the following site:

www.lists.apple.com

Consider obtaining some of these reference materials. They contain background information, explanations of basic concepts, and ideas for getting the most out of your network.

- *Teach Yourself Networking Visually*, by Paul Whitehead and Ruth Maran (IDG Books Worldwide, 1998).
- *Internet and Intranet Engineering*, by Daniel Minoli (McGraw-Hill, 1997).

In addition, NetworkMagazine.com offers a number of online tutorials on their Web site:

www.networkmagazine.com

If You're an Experienced Server Administrator

If you're already familiar with network administration and you've used Mac OS X Server, Linux, UNIX, or a similar operating system, you may find these additional references useful.

- A variety of books from O'Reilly & Associates cover topics applicable to Mac OS X Server, such as *Internet Core Protocols: The Definitive Reference*, *DNS and BIND*, and *TCP/IP Network Administration*. For more advanced information, see *Apache: The Definitive Guide*, *Writing Apache Modules with Perl and C*, *Web Performance Tuning*, and *Web Security & Commerce*, also published by O'Reilly and Associates. See the O'Reilly & Associates Web site:

www.ora.com

- See the Apache Web site for detailed information about Apache:

www.apache.org/

Although you'll want to use the administration tools provided with Mac OS X Server, it's possible to execute most UNIX commands and shell scripts from the built-in command-line interface of the Terminal application. You can access the command-line interface by logging in to the server as the administrator and navigating to the Terminal application, located in /Applications/Utilities. See Appendix A, "Advanced Topics," on page 301 for several suggestions.

Directory Services

What Are Directory Services?

Your Mac OS X Server uses directory services to find information about users. The server needs user information for authentication and to support various services.

User Information Needed for Authentication

When a user logs in to a Mac OS X Server, the server *authenticates* the user—or determines whether the user is a valid user. Only valid users are entitled to access a server or take advantage of the services it provides.

To authenticate a user, the server consults this information for the user:

- user name
- password
- user ID

At a minimum—regardless of the services your users will use—each user that you want to be able to access the server must have a user name, a password, and a user ID stored in a location accessible to the server. When a user logs in and enters a user name and password, the information entered must match one of the users defined for the server for the user to be authenticated.

Other User Information Needed by the Server

Other user information is needed by individual services. For example, mail service requires mail settings for each user, and Macintosh Management service needs to know a user's home directory. Most services require the user ID.

Appendix A, “Advanced Topics,” on page 301 describes all the data that individual services need to access after a user has been authenticated.

Where You Can Define User Information

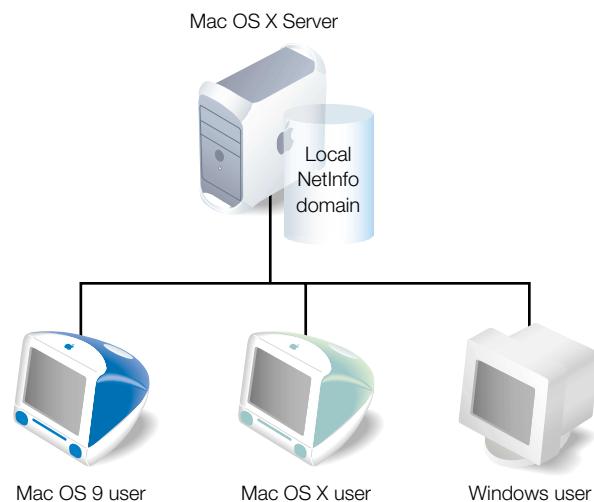
User information needed by directory services is stored on Mac OS X Servers in NetInfo databases. A NetInfo database is known as a *domain*.

Mac OS X Servers can also retrieve user information from standard servers known as Lightweight Directory Access Protocol (LDAP) servers. LDAP servers are often used to handle requests for user information.

Where you store your server's user information is determined by whether it needs to be shared.

If User Information on a Server Is Not Shared

When your server supports users whose information cannot be obtained from another Mac OS X Server on the network, information for users must reside locally, on the server itself. In this case, it is stored in a NetInfo domain—called the *local* domain—on the server:

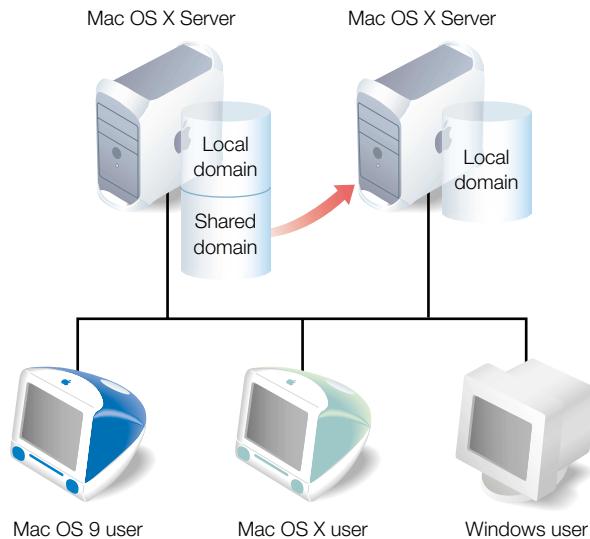


When a user logs in to the server, directory services search for the user in the local domain. The user can access the server only if the user is defined in the local domain.

Every Mac OS X Server has a local domain. Users defined in a local domain are visible only to the computer on which the domain resides. While defining users in the local domain is adequate for standalone servers or servers used in simple networks, in many cases it is more efficient for computers to *share* user information. Sharing user data minimizes redundancy, so when a user's data changes, it needs to be changed in fewer places.

If User Information on a Server Can Be Shared

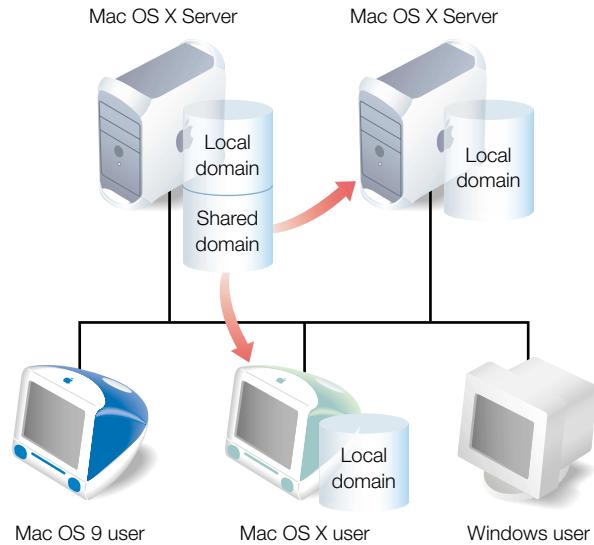
When your network has several Mac OS X Servers that provide services for users, user information stored in a NetInfo domain on one of the servers can be *shared* among the servers:



You define a shared domain when NetInfo information needs to be visible from multiple Mac OS X Servers.

In the picture above, users who are defined in the shared domain can access both servers. When a user logs in to either server, directory services search for the user in the local domain on that server. If the user is not found, directory services look for the user in the shared domain.

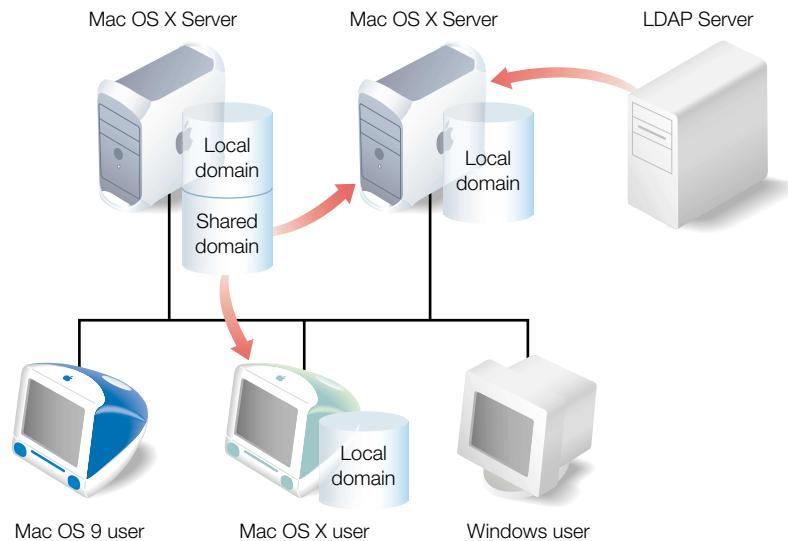
A shared domain can also be used to manage who can use a computer running Mac OS X:



Like Mac OS X Server, a computer running Mac OS X always has a local NetInfo domain. In the picture above, users who are defined in the Mac OS X local domain *or* in the shared domain on the server can use the Mac OS X computer.

If Information External to the Server Can Be Shared

Some organizations—such as universities and worldwide corporations—maintain user information on LDAP servers. Your Mac OS X Server can be configured to retrieve user information from these standard systems:



When a user logs in to one of the Mac OS X Servers, directory services still search for the user in NetInfo domains, starting with the local domain. But if the user is not found and the server has been configured to use an LDAP server, the server consults the LDAP server for information about the user.

How the Server Finds User Information

Directory services, which are part of the underlying architecture of a Mac OS X Server, provide a centralized roadmap that the server uses to find information about users, groups (collections of users), and devices—all the people and resources your server supports.

When your server needs user information, directory services identify where the server should look for that information:



When your server needs to access user information stored in multiple locations, such as NetInfo domains on different servers and one or more LDAP servers, directory services also control the *order* in which the server searches those locations.

The locations searched and the order in which they are searched are called a server's *search policy*. When a user logs in, directory services look for the user in the local NetInfo domain, then possibly in a shared domain or LDAP server, depending on how the search policy has been set up.

Using NetInfo

NetInfo lets you store and manage user information on a Mac OS X Server.

There's always at least one NetInfo domain defined on a server—the *local* domain.

Information stored in the local domain is visible only to the server on which it resides. It cannot be shared with other servers. So users defined in the local domain have access only to the server on which the local domain resides.

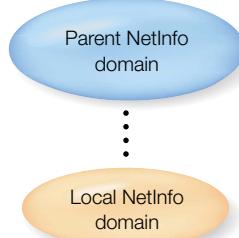
If you want to share information in a NetInfo domain, you need to make the local domain a *child* of a shared domain, called the *parent* domain.

Before You Set Up NetInfo

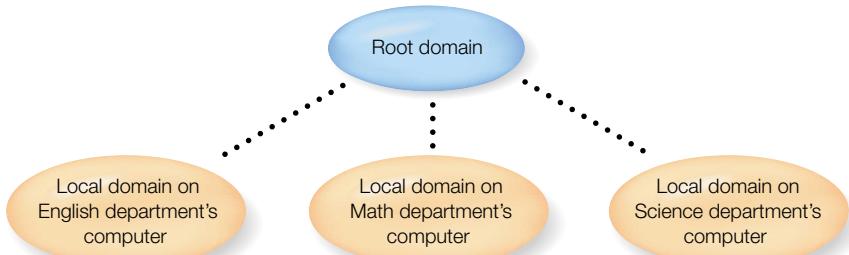
If you think you can take advantage of shared NetInfo domains, you need to understand parent-child hierarchies.

Two-Level Hierarchies

The simplest hierarchy is a two-level hierarchy:

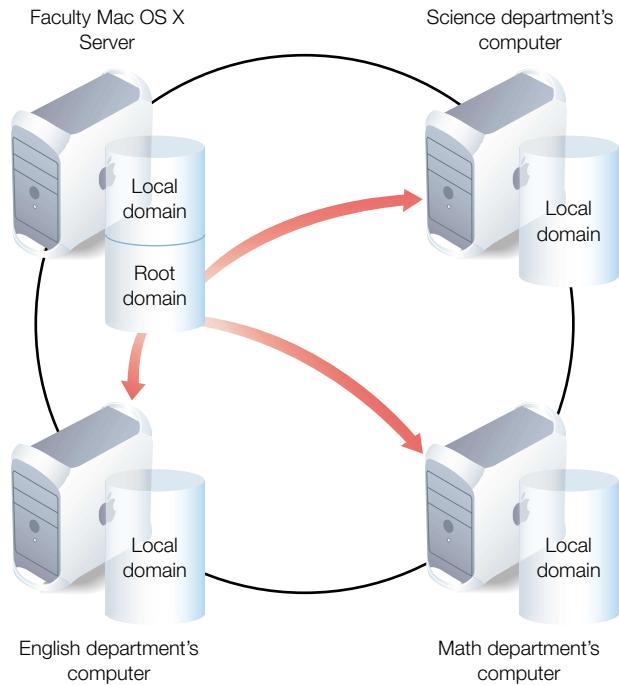


Here's a scenario in which a two-level hierarchy might be used:



Each department (English, Math, Science) has its own computer. The students in each department are defined as users in the local domain of that department's computer. All three of these local domains have the same parent—the root domain—in which all the instructors are defined. Instructors, as members of the root domain, can use services on *all* the departmental computers. The members of each local domain can only use services on the server where their local domain resides.

While local domains reside on their respective servers, a parent domain can reside on any Mac OS X Server accessible from the child domain's computer. In this example, the root domain can reside on *any* server accessible from the departmental servers. It can reside on one of the departmental servers, or—as shown here—on an entirely different server on the network:

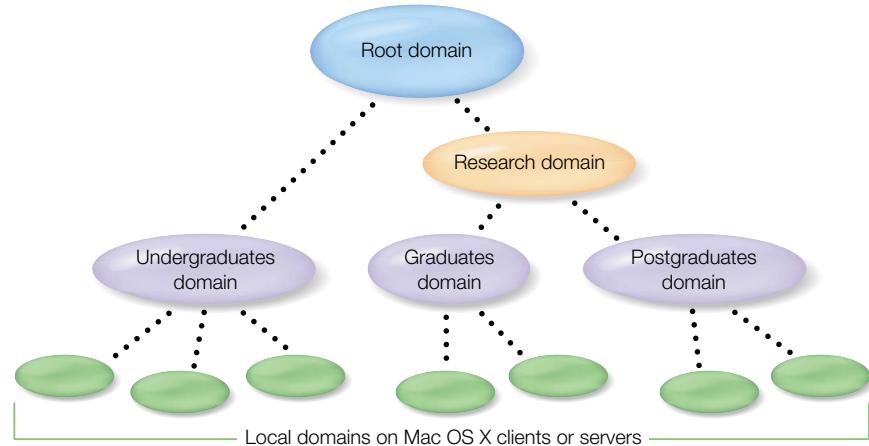


When an instructor logs in to any of the three departmental servers and cannot be found in the local domain, the server searches the root domain.

A root domain is a special kind of shared domain. It is the shared domain that is always at the top of a NetInfo hierarchy. It is visible to all computers that use the hierarchy. In this example, the root domain is the only shared domain, but in more complex hierarchies, there may be many shared domains.

More Complex Hierarchies

NetInfo also supports multilevel domain hierarchies. Complex networks with large numbers of users may find this kind of organization useful, although it's much more complex to administer.



In this scenario, an instructor defined in the root domain can use Mac OS X computers on which any of the local domains reside. Research fellows, defined in the Research domain, can log in to any Mac OS X computers whose local domains have the Graduates or Postgraduates domain as their parent, because the Research domain is the parent of the Graduates and Postgraduates domains.

How a Server Searches Through NetInfo Hierarchies

The *default* search strategy for a server is to search for a user in NetInfo domains, starting with the local domain:

- If the server's local domain has no parent, the server searches only the local domain.
- If the server's local domain does have a parent NetInfo domain, the server searches the parent domain when a user is not found in the local domain. If the user is not found in the local domain's parent and that parent domain is configured as the child of a second parent domain, the second parent is searched. If the user is still not found, the server continues searching up through the NetInfo hierarchy, stopping when the user is found or after the final parent has been searched.

If you want your server to search other NetInfo domains, or if you want to specify that LDAP servers be searched, use the Directory Setup application to customize the search policy, as described in “Setting Up Search Policies” on page 52.

Setting Up NetInfo for the First Time

Follow these steps to set up your NetInfo domains:

Step 1: Assess your server access requirements

Identify which users need to access your Mac OS X Servers.

Users whose information is not accessible from an LDAP server, or whose information can be managed most easily on a Mac OS X Server, should be defined in a NetInfo domain.

Step 2: Design the NetInfo hierarchy

Determine whether user information should be stored in a local NetInfo domain or in a NetInfo domain that can be shared among servers. Design your NetInfo hierarchy, identifying the shared and child domains you want to use, the servers on which the shared domains should reside, and the parent-child relationship between domains. In general, try to limit the number of users associated with any domain to no more than 10,000.

Chapter 2, “NetInfo Planning,” in *Understanding and Using NetInfo* provides some guidelines that will help you decide what your NetInfo hierarchy should look like.

Step 3: Set up the NetInfo hierarchy

These are the main steps for setting up NetInfo hierarchies:

- 1** Set up shared domains. On each server you want to host shared domains, you create them and configure them so that they bind together into the hierarchy you want.
- 2** Set up local domains on each Mac OS X computer so that they bind to the shared domain you want to act as the parent domain.
- 3** Set up replication. You can replicate shared domains to improve reliability and speed of access to their data.
- 4** Set up Windows user authentication. If Windows users need to be authenticated using NetInfo and encrypted passwords, you enable Authentication Manager in all the domains in the NetInfo hierarchy.
- 5** Populate shared domains with users, groups, and other information you want to share.

Chapter 3, “Setting Up NetInfo Hierarchies,” in *Understanding and Using NetInfo* describes what to do in each of these steps.

Step 4: Customize your search policy (optional)

If the default NetInfo search policy for a server is not adequate for your purposes, use Directory Setup to customize the search policy, as described in “Setting Up Search Policies” on page 52.

Using LDAP

Your server's built-in LDAP support lets it retrieve user information from an LDAP V2 server.

LDAP servers can maintain information for a wide variety of individuals or network resources, including users, groups, printers, or servers. Once an LDAP server has been set up, you can easily configure your Mac OS X Server to access it to retrieve user and other information.

Before You Set Up LDAP Server Access

Before it can serve as a resource for Mac OS X Server user information, an LDAP server must be configured to support LDAP-based authentication and password checking. The system administrator responsible for maintaining the LDAP server and its data should configure the LDAP server for access.

To provide the appropriate information for user authentication, the LDAP server must contain entries and attributes for four items: user name (in RecordName and RealName fields), password, and user ID. Depending on which Mac OS X Server services a user will need access to, additional information may also be required.

After the LDAP server is configured to supply all needed data, make a note of the search base and attribute name of each data item. You will need this information when configuring your Mac OS X Server for LDAP access.

Setting Up LDAP for the First Time

Follow these steps to configure your server to access an LDAP server; see “Configuring LDAP Access” on page 323 for more details.

Step 1: Prepare LDAP server data

Modify the LDAP server entries and attributes as necessary to provide the data needed for server authentication, and for the other services that will use the data. “LDAP Data Specifications” on page 314 provides complete specifications for LDAP data that's used by Mac OS X Servers. It may be necessary to add, modify, or reorganize information in your LDAP server to provide the information in the format needed.

Step 2: Enable LDAP support

Open the Directory Setup application (located in Applications/Utilities). Click the lock and log in as server administrator. Select LDAPv2 in the Directory Setup Services pane, then click Configure.

Step 3: Identify the LDAP server

In the Identity pane, specify the LDAP server's domain name or IP address.

Step 4: Define the LDAP search base

In the Records pane, map the record type “Users” to one or more search bases on the LDAP server that provide user information (for example, o=people, ou=your company name). Also map the record type “Groups” if you will be retrieving group information from the LDAP server.

Step 5: Map the data types for user and group information

In the Data pane, map at least the data types RecordName, RealName, Password, and UniqueID to the LDAP fields that will supply values for them. For example, UniqueID may be stored in an LDAP field named userid. If other information will be retrieved, map additional data types as needed.

Step 6: Define the connection attributes

In the Access pane, enter information about the connections established between your server and the LDAP server, such as the maximum time to spend searching for data on the LDAP server.

Step 7: Indicate how you want to use LDAP data

Either add the LDAP server to the server’s search policy or define aliases for specific users on the LDAP server. “Setting Up Search Policies,” next, tells you how.

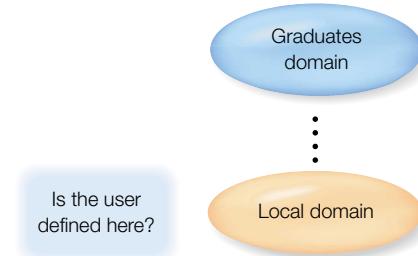
Setting Up Search Policies

A server looks for user information in the locations specified in the server’s search policy.

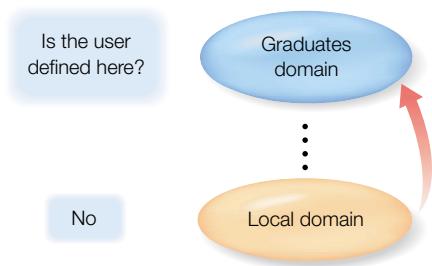
If you are using only NetInfo domains to store user information, the default search policy is usually sufficient. But when you want to search LDAP servers or additional NetInfo domains, you define a custom search policy by using Directory Setup.

The Default Search Policy

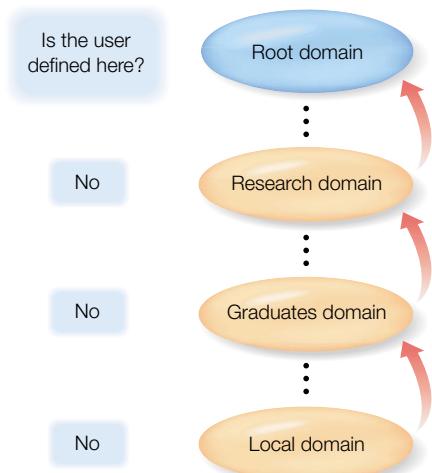
Your Mac OS X Server *always* searches its local NetInfo domain when a user tries to log in.



If a user is not found in the local domain, any parent domain defined for the local domain is searched:

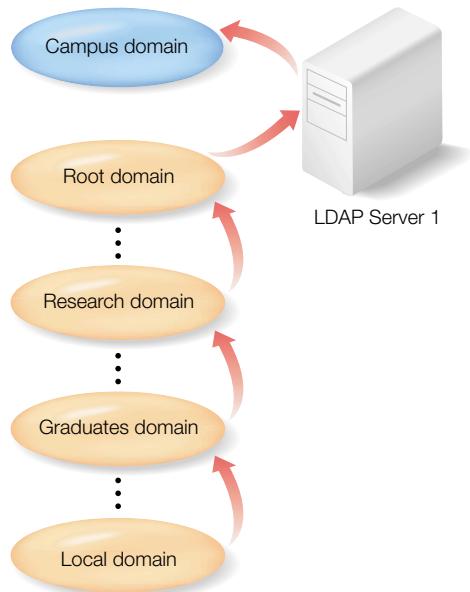


If the user is still not found, the next parent in the NetInfo hierarchy is searched, and so on until the root domain is searched:



Custom Searches

When you want to use an LDAP server or NetInfo domains that aren't in the default search policy to obtain information about users, you set up a custom search policy using the Directory Setup application. Here's an example custom search policy:

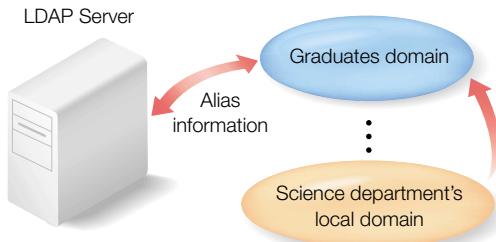


In this scenario, LDAP Server 1 is consulted for user information when a user cannot be found in the domains of the default search policy. If the user's information is not found on the LDAP server, a NetInfo domain named "Campus" is searched.

Using Aliases

Sometimes you'll want a server to be able to authenticate a user whose information is not stored in any of the locations specified in a search policy.

Your server can locate the information for such a user if you define an alias for the user in one of the NetInfo domains that *is* in the search policy. An alias is a pointer to the location where the user's information is actually stored. When the server needs to authenticate a user using an alias, it retrieves the user's information from the actual location where it resides. See the following illustration:



In the picture above, an alias for a user has been defined in the Graduates domain. The alias is used to retrieve information for the user from an LDAP server. The entire LDAP server does not need to be searched when a user is not found in the local or Graduates domain. A search is conducted only for the user the alias refers to.

To set up a scenario such as this one, you would configure your server to access an LDAP server but *not* add the LDAP server to the search policy. Then you would create aliases for individual users on the LDAP server in a NetInfo domain that *is* in the search policy.

You create aliases using the Users & Groups module of Server Admin. For more information, see the onscreen help for Users & Groups.

Before You Set Up Your Search Policy

Before you define a server's search policy, make sure any NetInfo domain or LDAP server you want the server to search has been configured for access by the Mac OS X Server.

Also determine whether defining aliases in one or more of your NetInfo domains would be useful for individual users.

Setting Up Search Policies for the First Time

Step 1: Determine whether the default search policy is sufficient

If the default NetInfo search policy is adequate for your environment, you're done. Otherwise, go to step 2.

Step 2: Open Directory Setup

The Directory Setup application is located in Applications/Utilities.

Step 3: Define a search policy option for the server

In the Authentication pane, use the Search pop-up menu to choose the search policy you want to set up:

- “NetInfo network” is the default NetInfo search policy used when a parent NetInfo domain has been configured for the server. Servers using this policy look for a user’s information in the local domain first, then proceed through the hierarchy of parent domains.
- “Local directory” causes the server to search for users *only* in the local NetInfo directory.
- “Custom path” lets you specify locations to search after the server searches NetInfo domains in the default NetInfo search policy. Select LDAP servers that have been configured for the server, or NetInfo domains that aren’t in the default search policy. See “Configuring LDAP Access” on page 323 for details.

Step 4: Define a search policy for personal applications (optional)

In addition to setting up the search policy for the server, you can define a search policy for use by your personal applications, such as mail or personal information managers. To do so, use the Contacts pane and the procedure described in step 3.

Users and Groups

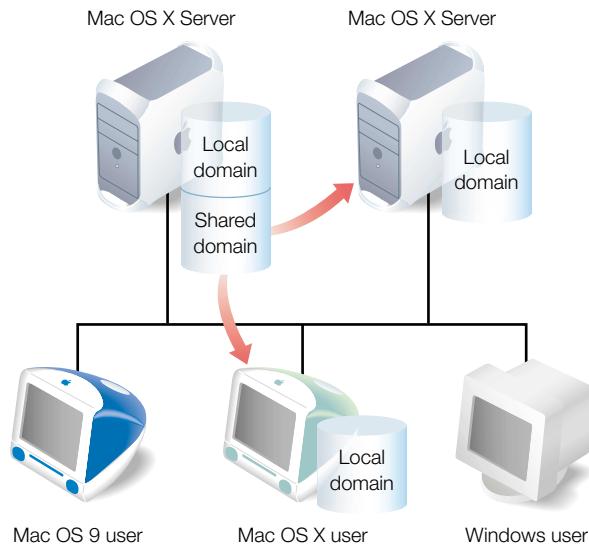
What Are Users and Groups?

To give individuals or groups (collections of individuals with similar requirements) access to your Mac OS X Server and to the services it hosts, you define users and groups.

This chapter summarizes the attributes of users and groups and tells you how to set them up.

How User Information Is Used

Your Mac OS X Server uses information you define for users to authenticate them and determine whether they are authorized to use particular services. User information is stored in NetInfo databases, known as *domains*:



Every Mac OS X computer and Mac OS X Server has a local domain. Users defined in a local domain can only use the computer where the local domain resides. In the preceding illustration, users defined in the local domain on a server only have access to that server. And users defined in the local domain on a Mac OS X computer can only log in to that computer.

Mac OS X Servers can also have shared domains defined on them. A shared domain stores user information that can be used by *multiple* Mac OS X computers and servers on a network. If a user is defined in a shared domain, he or she can use any computers that are configured to retrieve user information from that domain. In the preceding illustration, users defined in the shared domain can log in to either server or to a Mac OS X computer. If a user is not found in the local domain when the user logs in, the shared domain is consulted.

You use the Users & Groups module in Server Admin to define users and groups in a server's local and shared domains.

You can also configure a server to retrieve user information from Lightweight Directory Access Protocol (LDAP) servers. See "Using LDAP" on page 51 for more information if you are using or plan to use an LDAP server.

Characteristics of Users

When you define a user, you specify the information needed to authenticate the user: user name, password, and user ID. Regardless of the services a user will be using, this information is required. When the user logs in, the user name and password entered by the user must match one of the users defined for the server for the user to be authenticated.

Other information stored for users is needed by individual services—to determine what the user is authorized to do and perhaps to personalize the user's environment. For example:

- A user's server access information determines whether the user can administer the server. Only users with administrator privileges can use Server Admin and the other server administration applications.
- A user's mail information describes the user's mail account attributes, which are used by mail service (page 153).
- Macintosh Management service (page 195), Web service (page 121), Apple file service (page 85), and Network File System service (page 100) use home directory information for a user. A home directory is a network location where a user's files and preferences are stored.

Characteristics of Groups

A group is simply a collection of users who have similar needs. For example, you can add all English teachers to one group and give the group access privileges to certain files or folders on the Mac OS X Server.

Groups simplify the administration of shared resources; instead of granting access to those resources to each individual who needs them, you can simply add the users to a group, and grant access to the group.

Before You Set Up Users and Groups

Before setting up users and groups on one or more Mac OS X Servers:

- Devise a strategy for storing user information so that it is accessible to all Mac OS X Servers that need it. Set up any shared NetInfo domains or LDAP servers needed to implement that strategy, using the information provided in Chapter 2, “Directory Services.”
- If a server has multiple NetInfo domains, determine which users should be defined in each domain.

Note: If all the NetInfo domains have not been finalized when you are ready to start adding users, simply add them to any NetInfo domain that already exists on one of your servers. (You can always use the local domain—it’s always available.) You can easily move users and groups to another domain or server later using the Users & Groups module; instructions are in the onscreen help for Users & Groups.

- Identify users who have similar server requirements. You can add them to groups.

Setting Up Users and Groups for the First Time

To set up users and groups on your Mac OS X Server, complete the following steps. If you require additional help to perform any of these steps, click Users & Groups in Server Admin, then choose Help.

Step 1: Modify the administrator account defined at server setup

When you use the Setup Assistant to configure your server, you specify a password for the owner/administrator. The password you specify also becomes the root password for your server. Use the Users & Groups module in Server Admin to create an administrator user with a password that is different from the root password. Server administrators do not need root privileges.

The root password should be used with extreme caution and stored in a secure location. The root user has full access to the system, including system files. If you need to, you can use the Users & Groups module to change the root password. Choose Show Users & Groups List, then select Show System Users & Groups to work with the root user.

Step 2: Create new users

Use the Users & Groups module in Server Admin to create new user accounts. If the server has multiple NetInfo domains, be sure to select the domain where you want to create the user. See “User Settings,” next, for an explanation of user settings.

Step 3: Create new groups (optional)

Use the Users & Groups module in Server Admin to create new groups if you want to use them. If the server has multiple NetInfo domains, be sure to select the domain where you want to create the new group. See “Group Settings” on page 68 for an explanation of the group settings.

User Settings

To access the user settings, click the General tab in Server Admin. Then do any of the following:

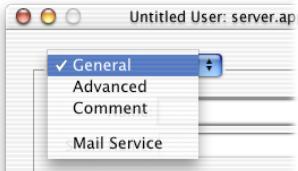
To create a new user:

- Click Users & Groups and choose New User. Then, if presented with a list of domains, choose the NetInfo domain in which you want to create the user.
- Click the New User button in any Users & Groups window in which it is available. (The new user will be created in the domain you are currently working with.)

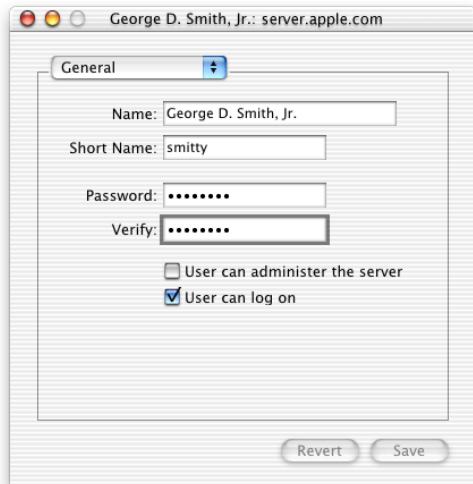
To edit a user:

- Select the user’s name in a window (for example, the U&G Find Results window) and click the Edit button.

The user settings window has four panes: General, Advanced, Comment, and Mail Service. Choose the pane you want to work with from the pop-up menu at the top of the window.



General User Settings



Name

Enter a name used to identify the user—for example, Bob W. Brown, Jr.

Short Name

Enter a short login name, which may also be used in an email address. It can contain only letters, numbers, the hyphen character (-), and the underscore character (_). Typically, this name contains 8 or fewer characters.

Password

Enter the user's password. The user enters this password when logging in to the server. The password is case-sensitive and does not appear on the screen as it is entered. The user can change the password when he or she logs in.

Use letters, numbers, and symbols in combinations that won't be easily guessed by unauthorized users. Avoid spaces and Option-key combinations. Also avoid characters that can't be entered on computers the user will be using. (Some computers do not support passwords that contain double-byte characters, leading spaces, embedded spaces, and so forth.) See “Mac OS X Server Password Restrictions” on page 71 for password requirements of specific services on your Mac OS X Server.

Verify

Use this field to reenter the password you entered in the Password field.

User can administer the server

Select this option if you want the user to be able to administer the server. When you first install Mac OS X Server, only the owner/administrator designated during server setup can administer it. Server administrators can use Mac OS X Server and other server administration applications, and they have full access to all the server's facilities.

User can log on

Select this option if you want the user to be able to log in to the server. It is selected by default. Deselecting this setting does not disable mail delivery to the user. To disable mail delivery, use the Mail Service pane.

Advanced User Settings



User ID

This is a number that uniquely identifies a user and determines the privileges the user has on a Mac OS X Server. For example, user IDs are used to manage privileges associated with share points; for more about privileges, see Chapter 4, “Sharing.”

The user ID is assigned automatically when a new user is created, but you can change it. Assign a value of 100 or greater that is unique within the server’s search policy. (The search policy is described in “Setting Up Search Policies” on page 52.) The maximum number is 2,147,483,647. User IDs below 100 are assigned to system accounts. Users with these IDs cannot be deleted and should not be modified.

Primary Group

Enter the ID of the group you want the user to automatically belong to. By default, it is 20.

Login Shell

Choose the default shell the user will use for command-line interactions with the server. The option None, which prevents a user from using the command line, is useful if you want to make sure a user cannot access the server using SSH.

Home Directory

Define the user's home directory. This is a folder for a user's personal use. It is displayed automatically when the user chooses Home from the Finder's Go menu. It must be located within a special directory known as a *share point*.

Before you define a home directory, the share point in which you want it to reside must exist. You can use the default share point for home directories (Users) or create a different share point. Make sure that the share point owner has Read & Write privileges and that Group and Everyone have Read privileges. See Chapter 4, "Sharing," for information about share points and privileges and to Users & Groups Help for instructions on creating a share point for home directories.

When you initially define a user, the default home directory settings are assigned to the user. (You can define the default home directory settings using the Home Directory Defaults command in the Users & Groups menu.) You can override the default settings for each individual user if you like:

- Choose None to give the user no home directory.
- Choose Local to create a home directory on the server where the user is defined. The directory will have the same name as the user's short name and will reside in the share point you choose from the Share Point pop-up menu. If the share point is Users, the home directory for a user named Mary might be the folder Users/Mary. The home directory name is displayed next to Path, under the Share Point pop-up menu.



The path to the home directory relative to the share point is displayed beneath the home directory name.

When Server Admin creates the home directory, the user is defined as the owner of the home directory and assigned Read & Write privileges.

- Choose Custom if you want to define a home directory on a different server or if you want full control over the home directory path and name.

Important Server Admin automatically creates home directories only on the server you are logged in to. If you want a user's home directory to reside on a remote server, create the home directory manually before using the Advanced pane to associate a user with the home directory. Onscreen help tells you how to define home directories manually.

The Custom option is useful, for example, if you want to organize home directories into several subdirectories within a share point. If Users is the share point, and home directories for teachers and students are grouped into subdirectories named Teachers and Students, a teacher's home directory might be Users/Teachers/Smith, and a student's home directory might be Users/Students/Mary. Because the home directories are not at the top level within the share point, you would use the Custom option to define them.



Enter the server's DNS name or IP address in the Server field and the share point in the Share Point field. In the Path field, enter the home directory folder name preceded by the path to it within the share point. The path to the home directory relative to the share point is displayed beneath the Path field.

After using the Custom option to create a home directory on the local server, use the Sharing module to define the user as the owner of the home directory, and assign the owner Read & Write privileges. Refer to Chapter 4, “Sharing,” for information about defining privileges.

You can configure home directories to be visible automatically to network users. See “Setting Up Home Directories to Mount Automatically” on page 70 for instructions.

User Comment



You can use the Comment pane to enter general information about the user. Comments can be as long as 32,767 characters.

Mail Service Settings

The Mail Service pane lets you enable and disable the user’s access to mail and configure settings for the user’s mail account. See Chapter 8, “Mail Service,” for complete information about how these settings are used to provide mail services for a user.

Disabling Mail

To disable mail delivery for the user, click None.



Enabling Mail

To enable mail delivery for the user and set mail account options, click Enable.



Mail Account located on server

Enter the IP address or DNS name of the server to which the user's mail is routed.

Select the access method of the account

Select the protocol used for the user's mail account: Post Office Protocol (POP) and/or Internet Message Access Protocol (IMAP). Chapter 8, "Mail Service," provides information about these protocols.

Options

Click to set additional mail account options:



Use separate inboxes for POP and IMAP

Select this option to manage POP and IMAP mail using different inboxes.

Show POP mailbox in IMAP folder list

Select this option to show an IMAP folder named "POP Inbox."

Enable NotifyMail

Select this option to automatically notify the user's mail application when new mail has arrived. The IP address to which the notification is sent can be either the last address from which the user logged in or an address you specify.

Forwarding Mail

You can automatically forward a user's mail to a particular email address by clicking Forward and specifying the address.



Group Settings

To access the group settings, click the General tab in Server Admin, then do any of the following:

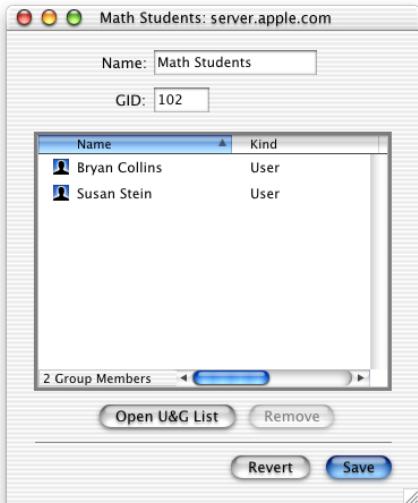
To create a new group:

- Click Users & Groups and choose New Group. Then choose the domain in which you want to create the new group if presented with a list of domains.
- Click the New Group button in any Users & Groups window in which it is available. (The new group will be created in the domain you are currently working with.)

To edit a group:

- Select the group's name in a window that lists groups (for example, the U&G Find Results window) and click the Edit button.

This is the window you use to work with group settings.



Name

Enter a name for the group. If you want to be able to send mail to the group, the name should not include the space character or Option-key characters.

GID

This is the group's ID, used to determine what members of the group can do on the server. For example, the group ID is used internally to keep track of privileges associated with share points. For more about privileges, see Chapter 4, “Sharing.”

The group ID is assigned automatically when a new group is created, but you can change it. Assign a value greater than 100 that is unique within the NetInfo domain you are working with. Groups with IDs below 100 cannot be deleted.

Name, Kind, ID, and Location

These are characteristics of users currently associated with the group. “Kind” lists “Administrator” if the user has administrator rights; otherwise it lists “User.” “Location” identifies the NetInfo domain in which the user is defined. You may need to scroll horizontally to see all these columns.

To add a user to the group, click Open U&G List, then drag the user from the Users & Groups List into the group settings window. To remove a user from the group, select the user, then click Remove.

Users and Groups Strategies and Tips

This section provides some techniques that can be used to help you manage your users and groups.

Exporting and Importing Users and Groups

On some occasions you may need to put information for users or groups in a text file, then add users and groups from the file instead of adding them individually. This approach is useful, for example, when you want to add the same users and groups to multiple servers that aren't on the same network.

You can use the Users & Groups module to import the users and groups from the file into a NetInfo domain on any Mac OS X Server. To create the file, you have two options:

- The Users & Groups module can automatically create the file for you. This process is known as *exporting* users and groups.
- You can also create the file by hand. “File Format for Importing or Exporting Users and Groups” on page 308 describes the format of the file and provides instructions.

For additional instructions on using the Users & Groups module to import and export users and groups, see the onscreen help.

Setting Up Home Directories to Mount Automatically

A user's home directory is automatically visible when the user chooses Home from the Finder's Go menu.

You can also make home directories visible automatically to network users. Follow these steps to set up home directories to mount automatically for network users:

Step 1: Configure NetInfo

Create a shared NetInfo domain on the server where you want to store home directories. The domain must be in the search policy of Mac OS X computers on which you want automatic mounting to be available. See Chapter 2, “Directory Services,” for information about defining NetInfo domains and search policies.

Step 2: Set up a share point on the server

Use the Server Admin Sharing module to create a share point on the server and set it up for mounting automatically (page 80). See onscreen help for specific instructions.

Step 3: Make sure that users will not be automatically disconnected

Use the Server Admin Apple file service module to make sure that users will not be automatically disconnected when they do not use the server for a while. In the Idle Users pane, do *not* select “Disconnect idle users after _ minutes.” See page 90 for more information about this setting.

Step 4: Define users and their home directories

Use the Server Admin Users & Groups module to define users and aliases, if needed, in the shared NetInfo domain created in step 1. When setting up the user home directories, choose the share point configured in step 2.

Mac OS X Server Password Restrictions

Most of the Mac OS X Server applications and services that require passwords support 7-bit or 8-bit ASCII passwords without leading or trailing spaces. Use the following table to determine whether you need to take these restrictions into account when defining passwords for server users:

Service or application	7-bit ASCII passwords OK	8-bit ASCII passwords OK	Double-byte passwords OK
Apple file service	X	X	
File Transfer Protocol (FTP) service	X		
IMAP	X	X (some IMAP clients)	
Macintosh Manager	X	X	
POP3	X		
Server Admin	X	X	
Web service	X		
Windows services	X		

Solving Problems With Users and Groups

If users can't access files in their home directories:

Ensure that users have access to the share point in which their home directories are located and to their home directories. Users need Read access to the share point and Read & Write access to their home directories.

If a Mac OS X user defined in a shared NetInfo domain can't log in:

This problem occurs when a user tries to log in to a Mac OS X computer using an account in a shared NetInfo domain, but the server hosting the domain isn't accessible. The user can log in to the Mac OS X computer by using the local user account created automatically when he or she set up the computer to use a NetInfo account. The user name is "administrator" (short name is "admin") and the password is the NetInfo password.

Sharing

What Is Sharing?

The Sharing module in Mac OS X Server allows you to designate the information you want to share with others and assign access privileges to control who can see and use the information.

Shared items are contained within one or more *share points*. A share point is a folder, hard disk (or hard disk partition), or CD accessible over the network. It's the point of access at the top level of a group of shared items. Users see share points as volumes mounted on the desktop, or as volumes in the Finder in Mac OS X.

Privileges are the access levels you assign to any items you want to share with users. You'll use the Sharing module of Server Admin to set up share points and privileges that are used by other services such as Apple file service, Windows services (SMB), Network File System (NFS) service, and File Transfer Protocol (FTP) service.

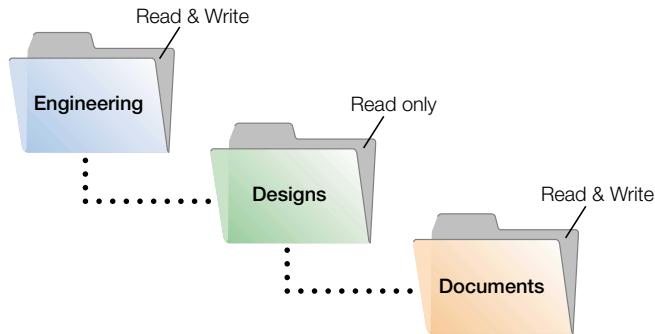
Note: QuickTime Streaming Server and Web service have their own privileges settings. You can read more about QuickTime Streaming Server in Chapter 9. You'll find information on Web privileges in "Access Settings for Web Sites" on page 134.

Before You Assign Privileges

Before you assign privileges, you need to understand how privileges for shared items work. You also need to consider which users need access to shared items, and what type of privileges you want those users to have.

Explicit Privileges

Share points and shared items (including files) have their own individual privileges. If you move an item to another folder, it retains its own privileges and doesn't automatically adopt the privileges of the folder where you moved it. In the following illustration, the second folder (Designs) and the third folder (Documents) were assigned privileges that are different from those of their “parent” folders:



Types of Privileges

There are four types of privileges that you can assign to a share point, folder, or file: Read & Write, Read Only, Write Only, and None. The table below shows how the privileges affect user access to different types of shared items (files, folders, and share points).

Users can	Read & Write	Read only	Write only	None
Open a shared file	Yes	Yes	No	No
Copy a shared file	Yes	Yes	No	No
Edit a shared file's contents	Yes	No	No	No
Open a shared folder or share point	Yes	Yes	No	No
Copy a shared folder or share point	Yes	Yes	No	No
Move items into a shared folder or share point	Yes	No	Yes	No
Move items out of a shared folder or share point	Yes	No	No	No

You can assign Write Only privileges to a folder to create a *drop box*. The folder's owner can see and modify the drop box's contents; everyone else can only copy files and folders into it, without seeing what it contains.

User Categories

You can assign access privileges separately to three categories of users:

Owner

A user who creates a new item (file or folder) on the file server is its owner, and automatically has Read & Write privileges to that folder. The owner of an item and the server administrator are the only users who can change its access privileges. The administrator or the item's owner can transfer ownership of the shared item to another user.

Group

You can put users who need the same access to files and folders into group accounts. Only one group can be assigned access privileges to a shared item. For more information on creating groups, see Chapter 3, “Users and Groups.”

Everyone

Everyone is any user who can log in to the file server: registered users, guests, anonymous FTP users, and Web site visitors.

Privileges Hierarchy

If a user is included in more than one category of users, each of which has different privileges, these rules apply:

- Group privileges override Everyone privileges.
- Owner privileges override Group privileges.

For example, when a user is both the owner of a shared item and a member of the group assigned to it, the user has the privileges assigned to the owner.

Client Users and Privileges

Users can set some privileges for files or folders that they create on the server, or in shared folders on their desktops. Users of AppleShare Client software can set access privileges for folders they own. Windows file sharing users can set folder properties, but not privileges.

Security Issues

Security of your data and your network is critical. The most effective method of securing your network is to assign appropriate privileges for each file, folder, and share point as you create it.

Be careful when creating and granting access to share points, especially if you’re connected to the Internet. Granting access to Everyone, or to World (in Network File System service) could potentially open up your data to anyone on the Internet.

Restricting Access by Unregistered Users (Guests)

When you configure any file service, you have the option of turning on guest access. Guests are users who can connect to the server anonymously without entering a valid user name or password. Users who connect anonymously are restricted to files and folders with privileges set to Everyone.

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, you can take these precautions using the Sharing module of Server Admin:

- Share individual folders instead of entire volumes. The folders should contain only those items you want to share.
- Set privileges for Everyone to None for files and folders that guest users should not access. Items with this privilege setting can only be accessed by the item's owner or group.
- Put all files available to guests in one folder or set of folders. Assign the Read Only privilege to the Everyone category for that folder and each file within it.
- Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder. You should also check this folder frequently for changes and additions, and check the server for viruses regularly with a virus-protection program.
- Check folders frequently for changes and additions, and check the server for viruses regularly with a virus-protection program.
- Disable anonymous FTP access using the FTP module of Server Admin.
- Don't export NFS volumes to World. Restrict exports to a specific set of computers.

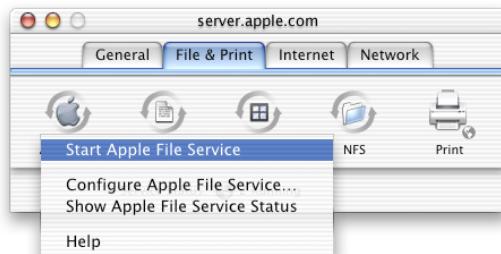
Setting Up Sharing for the First Time

You use the Sharing module of Server Admin to create share points and shared items, and to set privileges for them. When you set privileges, you also need to use the Users & Groups module of Server Admin to find groups.

The following steps tell you what to do to set up sharing for the first time. If you require additional help to perform any of these steps, click Sharing in Server Admin, then choose Help.

Step 1: Turn file service on

If you are administering the server remotely and want to select share points and set privileges, Apple file service must be running. If you're not sure if it's running, you can check easily. In Server Admin, click the File & Print tab. A service that is running has a globe on its icon. If you don't see the globe on the file service that you want, click the service icon, then choose the "Start" menu item.



Step 2: Create a share point

If you haven't already done so, create the item you want to share. You may want to partition a disk into volumes to give each volume different access privileges, or create folders that will have different levels of access.

To create a new folder, open the disk or folder where you want to place the new folder. Choose New Folder from the File menu and name the new folder.

Step 3: Set privileges for share points

Click the General tab, then click Sharing and choose Set Sharing Attributes. Select the item you want to share, then click Choose. The sharing window for the share point appears, where you can set the access levels you want.

To assign user and group access for a share point, click Users & Groups and choose Show Users & Groups List, or Find Users & Groups. If you choose Find, do a search for the user or group you want. Then drag the name to the appropriate field in the sharing window.

Choose the access privileges for Owner, Group, and Everyone from the pop-up menu next to each field. The privileges you assign are used by Apple file service, Windows services, and FTP service.

Sharing Settings

You set access privileges for share points in the sharing window. To access the sharing window, click Sharing in Server Admin. Then do one of the following:

- Choose Set Sharing Attributes, select an item, then click Choose.
- Choose Show Disks & Share Points, select an item, then click Privileges.

Choose General, Automount, or NFS Access Control from the pop-up menu to set privileges for a shared item. The settings available in each pane are described in the following sections.

General Settings

You use the General pane to set access privileges for share points and shared items.



Share this item and its contents

Select this option to set up the share point for AFP, Windows, and FTP access. To set it up for NFS access, see “NFS Access Control Settings” on page 81. You can share an item for either or both of these access strategies.

Owner

Drag a user from the Server Admin Users & Groups List to this field. The default owner is the person who created the item.

Group

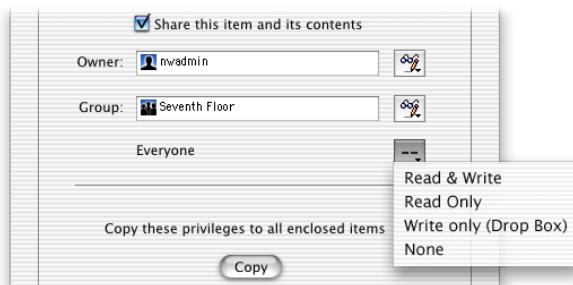
Drag a group from the Server Admin Users & Groups List. If you don't want any group to have access, set the Group access privileges to None.

Everyone

Everyone is any user who can log in to the file server: registered users, guests, anonymous FTP users, and Web site visitors. If you don't want everyone to have access, set the Everyone access privileges to None.

Privileges

Choose access levels for Owner, Group, and Everyone from the pop-up menu to the right of each user category.

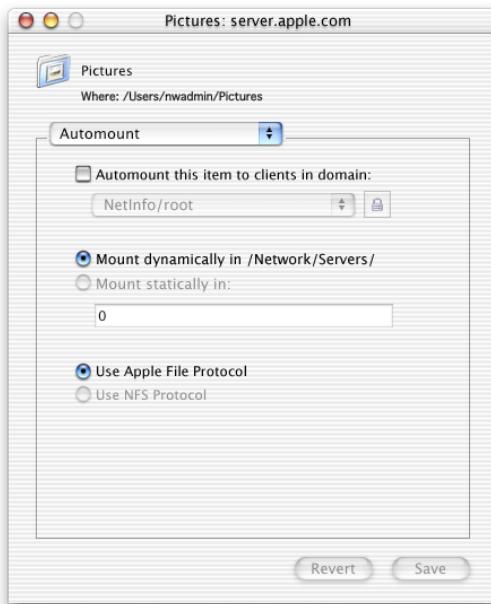


Copy

Click this button to copy this share point's privileges to all items (files and folders) contained in it. This will override privileges that other users may have set.

Automount Settings

You use the Automount pane to set up share points (not files) to mount automatically for Apple file service or NFS service. To access the Automount pane, select a shared item in the Disks & Share Points window and click Privileges. Then choose Automount from the pop-up menu below the share point name.



Automount this item to clients in domain

Choose the shared NetInfo domain to which you want to publish (or automount) this shared item. The share point will be mounted automatically on any computer configured to use the shared domain.

You are asked for the user name and password of a user authorized to change the domain. After you are authenticated, click “Automount this item to clients in domain.”

Mount dynamically in /Network/Servers

Select this option if you want client users to see share points in the /Network/Servers folder of their computer. When the user double-clicks a share point in the folder, the share point mounts on the user’s desktop or in the Finder (depending on the user’s System Preferences settings).

Mount statically in

Select this option if you want the share point to mount automatically when the client computer starts up. Choose the location where you want the item to appear. Do not use static mounts for home directories.

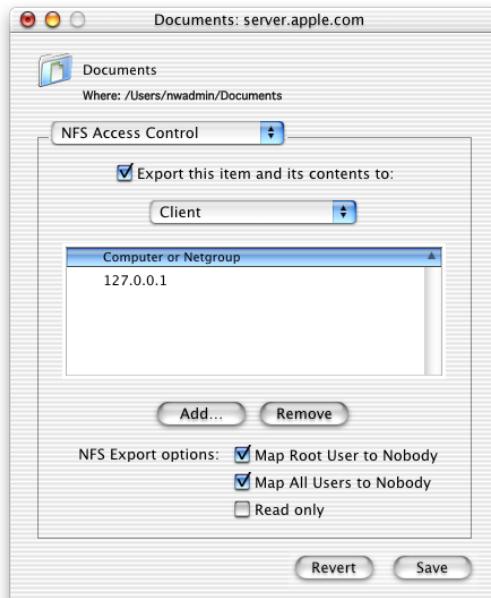
Automount options

If you've set up the share point for access using AFP and NFS, click one of the radio buttons to indicate which protocol you want to use to mount the share point.

NFS Access Control Settings

You use the NFS Access Control pane to set up Network File System (NFS) share point exports and access privileges for them. NFS handles authentication differently than other file services—it looks at IP addresses rather than user names and passwords to allow access. NFS share points are exported to valid client computers, and these exports are mounted as volumes in a location that you specify. NFS exports can also be Apple file service or Windows services share points, but they don't have to be.

To access the NFS Access Control settings, click Sharing and choose Set Sharing Attributes. Select the item you want to share, then click Choose. Choose NFS Access Control from the pop-up menu below the item name. For information about the settings, see page 102.



Solving Problems With Sharing

If users can't find a shared item:

Check the access privileges for the item. Users must have at least Read access privileges to the share point where the item is located, and to each folder in the path to the item.

Note: Server administrators don't see share points the same way a user does because administrators see everything on the server. To see share points from a user's perspective, log in using a user's name and password.

If users can't access a CD-ROM disc:

- Make sure you've made the CD-ROM disc a share point.
- If you share multiple CDs, make sure each CD has a unique name.

File Services

What Are File Services?

File services allow your client users to access files, applications, and other resources over a network. You use Server Admin to configure file services, turn them on and off, and check their status. You can turn on guest (unregistered user) access for each service using the module for that service, but to control access to the items you share, you use the Sharing module of Server Admin. For more information about sharing, see Chapter 4, “Sharing.”

Mac OS X Server includes four file services:

- Apple file service, which uses the Apple Filing Protocol (AFP), lets you share resources with clients who use Macintosh or Macintosh-compatible operating systems.
- Windows services use Server Message Block (SMB) protocol to let you share resources with clients who use Windows or Windows-compatible operating systems, and to provide name resolution service for Windows clients.
- Network File System (NFS) service lets you make directories (folders) available for your users who have NFS client software.
- File Transfer Protocol (FTP) service lets you share files with anyone using FTP.

Before You Set Up File Services

Security of your data and your network are the most critical issues you must consider when setting up your file services.

Setting File and Folder Privileges

The most important protection for your server is how you set the privileges for individual files. In Mac OS X, every file has its own privilege settings that are independent of the privileges for its parent folder. Users can set privileges for files and folders they place on the server, and the server administrator can do the same for share points. For more information about setting up share points and assigning access privileges, read Chapter 4, “Sharing.”

Restricting Guest Access

When you configure any file service, you have the option of turning on guest access. Guests are users who can connect to the server anonymously without entering a valid user name or password. Users who connect anonymously are restricted to files and folders with privileges set to Everyone.

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, you can take these precautions using the Sharing module of Server Admin:

- Share individual folders instead of entire volumes. The folders should contain only those items you want to share.
- Set privileges for Everyone to None for files and folders that guest users should not access. Items with this privilege setting can only be accessed by the item's owner or group.
- Put all files available to guests in one folder or set of folders. Assign the Read Only privilege to the Everyone category for that folder and each file within it.
- Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder. You should also check this folder frequently for changes and additions, and check the server for viruses regularly with a virus-protection program.
- Check folders frequently for changes and additions, and check the server for viruses regularly with a virus-protection program.
- Disable anonymous FTP access using the FTP module in Server Admin.
- Don't export NFS volumes to World. Restrict exports to a specific set of computers.

Allowing Access to Registered Users Only

If you do not want to allow guests to access your server, make sure guest access is turned off for each file service. If you see a checkmark next to Allow Guest Access in any service's module, guest access is turned on. Click the box to remove the checkmark and turn guest access off.

Apple File Service

Apple file service allows Macintosh client users to connect to your server and access folders and files as if they were located on the user's own computer. If you are familiar with AppleShare IP 6.3, you will find that Apple file service in Mac OS X Server functions in the same way. It uses a new version of the Apple Filing Protocol (AFP), version 3.0, which supports new features such as Unicode filenames and 64-bit file sizes.

One difference in the new Apple file service is that AppleTalk is no longer supported as a connection method. Clients using AppleTalk can use the Chooser to look for your server on the network, but they will use TCP/IP to connect.

Apple file service provides support for Unicode filenames, a standard that assigns a unique number to every character regardless of language or the operating system used to display the language.

Before You Set Up Apple File Service

If you turn on Apple file service in the Mac OS X Server Setup Assistant, your server will be available right away on the network. However, no users can connect to it until you create share points with appropriate privileges and create authorized users. Read Chapter 4, "Sharing," and Chapter 3, "Users and Groups," to learn more about these topics.

Finding Compatible AppleShare Versions

Client computers must have AppleShare version 3.7 or later installed to access an Apple file server. You can go to the Apple support Web site at www.apple/support/ to find out the latest version of AppleShare client software supported by the client's version of the Mac OS.

Enabling AppleTalk on Client Computers

To find the Apple file server over AppleTalk (using the Chooser), client users must enable AppleTalk. To do this in Mac OS X, open System Preferences and click Network. In Mac OS 9 and earlier, use the AppleTalk control panel.

Setting Up Apple File Service for the First Time

If you asked the Setup Assistant to configure Apple file service when you installed Mac OS X Server, you don't have to do anything else to use Apple file service. However, you should check to see if the default settings meet all your needs. If you did not set up Apple file service when you installed Mac OS X Server, you can do so now.

Step 1: Configure Apple file service

In Server Admin, click the File & Print tab, then click Apple and choose Configure Apple File Service. Click each of the four tabs in the Apple File Service Settings window and make the settings you want. For a description of the available settings, see "Apple File Service Settings" on page 86.

Step 2: Start Apple file service

Click Apple and choose Start Apple File Service. A globe appears on the service icon when the service is turned on.

Step 3: Create share points and users and groups

You need to set access privileges for share points (shared folders and disks) that you want to make available on your server. You also need to assign privileges to the users and groups you want to access your information. You can find out how to do these tasks in Chapter 4, “Sharing,” and Chapter 3, “Users and Groups.”

Apple File Service Settings

To access the Apple file service settings, click the File & Print tab, then click Apple and choose Configure Apple File Service. Click each of the four tabs to see the settings in that pane. The settings available in each pane are described in the following sections.

General Settings

You use the General pane to set identifying information about your server, enable automatic startup, and create a login message. To access the General pane, click Apple and choose Configure Apple File Service.



Computer Name

Type the name you want users to see when using the Chooser or the Network Browser. The name you enter here must be unique among all computers connected to the network. If you leave this field blank, the server will register itself on the network using its IP address, and the server's DNS name will show in this field.

Start Apple File Service on system startup

Select this option to ensure that if the server is restarted after a power failure or other unexpected event, file services will be available. In most cases it's best to turn on this option.

Register with Network Service Location

Select this option if you want to allow users to see this server in the “Connect to Server” pane in Mac OS X or in the Network Browser in Mac OS 9. This option is available to client computers that have Mac OS 9 or later installed.

If you turn on this option, you must also enable IP multicasting on your network router. See Chapter 12, “Network Services,” for more information about Service Location Protocol (SLP) and IP multicast. See page 265 for information about client and router capabilities.

Logon Greeting

Type the message that you want users to see when they connect.

Note: If a user doesn't see the login greeting, upgrade the software on the user's computer. Client computers must be using AppleShare client software version 3.7 or later.

Do not send same greeting twice to the same user

Select this option if you only want users to see the login greeting once. If you change the message, users will see the new message the next time they connect to the server.

Access Settings

You use the Access pane to set up client connections and guest access. To find the Access pane, click Apple and choose Configure Apple File Service, then click the Access tab.



Allow Guest access

Select this option if you want to allow unregistered users to access the file server. Guest access is a convenient way to provide occasional users with access to files and other items for which the appropriate privileges have been set.

Maximum client connections (including Guests)

Select Unlimited if you do not want to limit the number of users who can be connected to your server at one time. If you are using your server to provide a number of services, you can improve performance by limiting the number of client connections. To do so, click the button below Unlimited and type the number of connections you want to set as a limit.

Maximum guest connections

Select Unlimited if you are allowing guest access and don't want to limit the number of guest users who can be connected to your server at one time. If you want to specify how many of your maximum client connections can be used by guests, click the button below Unlimited and type the number of connections you want to allow.

Allow clients to browse using AppleTalk

Select this option if you would like client users to be able to find your file server using the Chooser. To find the server using the Chooser, AppleTalk must be enabled on both the client computer and the server.

Encoding for older clients

Choose a character set for the server that matches the character set used by your client users. When Mac OS 9 and earlier clients are connected, the server converts filenames from the system's UTF-8 to the chosen set.

Logging Settings

You use the Logging pane to configure and manage logs for Apple file service. To access the Logging pane, click Apple and choose Configure Apple File Service, then click the Logging tab.



Enable Access Log

Select this option if you want to create an access log. The access log stores information about any of the events you select. The log file is limited only by the amount of available disk space. Of course, the more events you choose, the larger the log file. Consider your server's disk size when choosing events to log.

Archive every _ days

Select this option if you want to specify how often the log file contents are saved to an archive. After the number of days you specify, the server closes the log file, renames it to include the current date, then opens a new log file. You can keep the archived logs for your records, or delete them to free disk space when they are no longer needed. The default setting is seven days.

Select events to include in the access log

Select the events that you want Apple file service to log. Entries are logged each time a user performs one of the actions you select.

Error Log: Archive every _ days

Select this option if you want to specify how often the error log file contents are saved to an archive. After the number of days you specify, the server closes the log file, renames it to include the current date, then opens a new log file. You can keep the archived logs for your records, or delete them to free disk space when they are no longer needed. The default setting is seven days.

Idle Users Settings

You use the Idle Users pane to configure and administer idle user settings. “Idle users” are users who are connected to the server but haven’t used the server volume for a period of time. To access the Idle Users pane, click Apple and choose Configure Apple File Service, then click the Idle Users tab.



Allow clients to sleep _ hour(s)-will not show as idle

Select this option if you don’t want the server to disconnect client computers that are in sleep mode. Sleep is a state in which a client computer uses very little power. On computers with the Energy Saver software installed, users can set the computer to sleep after a period of inactivity.

Disconnect idle users after _ minutes

Select this option if you want to disconnect idle users after a specified time. This ensures that server resources are available to current users. In addition, it may prevent unauthorized users from using an unattended computer to access information on the network.

Except

Select the users that you want to exempt from being disconnected:

- Guests
- Registered users (any user who is not also an administrator or guest)
- Administrators
- Idle users who have open files

Important If you don't select the last option, any idle user (guests, registered users, or administrators) who has open files will be disconnected and will lose unsaved changes to their work.

Disconnect Message

Type the message you want users to see when they're disconnected. If you do not type a message, a default message appears stating that the user has been disconnected because the connection has been idle for a period of time.

Not all client computers can display disconnect messages.

Solving Problems With Apple File Service

If users can't find the file server:

- Make sure the network settings are correct on the user's computer and on the computer that is running Apple file service. If you can't connect to other network resources from the user's computer, the network connection may not be working.
- Make sure the file server is running. You can use a "pinging" utility to check whether the server is operating.
- If the user is searching for the server via AppleTalk (in the Chooser), make sure you've enabled browsing over AppleTalk in the Access pane of the Apple File Server Settings window, and that AppleTalk is active on both the server and the user's computer.
- Check the name you assigned to the file server and make sure users are looking for the correct name.

If users can't connect to the file server:

- Make sure the user has entered the correct user name and password. The user name is not case-sensitive, but the password is.
- Make sure logging in is enabled for the user in the Users & Groups module of Server Admin.
- Check to see if the maximum number of client connections has been reached (in the Apple File Service Status window). If it has, other users should try to connect later.
- Make sure the server that stores users and groups is running.
- Verify that the user has AppleShare 3.7 or later installed on his or her computer.
- Make sure IP filter service is configured to allow access on port 548 if the user is trying to connect to the server from a remote location. For more on IP filtering, see “IP Filter Service” on page 285.

Apple File Service Specifications

Maximum number of connected users, depending on your license agreement	Unlimited (hardware dependent)
Maximum volume size	2 terabytes
TCP port number	548
Log file location	/Library/Logs in the AppleFileService folder

Windows Services

Windows services in Mac OS X Server provide four services to Windows clients without requiring any additional software. These services are

- file service, which allows Windows clients to connect to the Mac OS X Server using Server Message Block (SMB) protocol over TCP/IP
- print service, which also uses SMB to allow Windows clients to print to PostScript printers on the network
- Windows Internet Naming Service (WINS), which allows clients across multiple subnets to perform name/address resolution
- browsing, which allows clients to browse for available servers across subnets

Windows services use Unicode (a standard that uses 16-bit identifiers for any possible character) to display the correct language for the client. Since older client computers don't use Unicode, Windows services support Samba code pages, which translate from the native Unicode to the language the user has specified.

Before You Set Up Windows Services

If you plan to provide Windows services on your Mac OS X Server, read the following sections for considerations you should keep in mind. You should also check the Microsoft documentation for your version of Windows to find out more about the capabilities of the client software.

What You Need to Support Windows Clients

To support your Windows clients, you only need your Mac OS X Server software. Unlike previous Apple server products, Mac OS X Server comes with built-in browsing and name resolution services for your Windows client computers. You can enable WINS on your server, or you can register with an existing WINS server.

Windows services in Mac OS X Server also provide Windows Master Browser and Domain Master Browser services. This means you no longer need a Windows server or a primary domain controller on your network to allow Windows users to see your server listed in the Network Neighborhood window. Also, your Windows clients can be located on a subnet outside of your server's subnet.

Ensuring the Best Cross-Platform Experience

Mac OS and Windows computers store and maintain files differently. For the best cross-platform experience, you should set up at least one share point to be used only by your Windows users. In addition, you can improve the user experience by following these guidelines:

- Use comparable versions of application software on both platforms.
- Modify files only with the application they were created in.
- Limit filenames to 31 characters.
- Don't use symbols or characters with accents in the names of shared items.

Windows User Password Validation

Mac OS X Server offers two techniques for validating Windows user passwords:

- *Encrypted password validation.* This is the preferred approach because it is the safest and because it is the default technique supported by Windows computers on a local area network (LAN). This technique transmits encrypted passwords between a Windows computer and Mac OS X Server.

To use encrypted password validation, you enable Authentication Manager for all domains in your NetInfo hierarchy and define an encryption key for each domain. When Authentication Manager is enabled, a `tim_passwd` property is stored in NetInfo user records. It can be decrypted to get the cleartext password using the encryption key, which is stored in a file on the server that is readable only by root.

- *Cleartext password validation.* Use this technique only when encrypted transmission of user authentication information is not important. Windows computers must be configured individually to support cleartext password validation. See the Windows documentation for information on how to set up cleartext password validation.

When you use cleartext password validation, passwords are not stored in a recoverable format. The NetInfo password value, associated with the `passwd` property, is derived using a one-way hash, which can't be easily decoded. The one-way hash ensures that each time it's used for the same password, the same result occurs.

To set up encrypted password validation, enable Authentication Manager on every Mac OS X computer that participates in the hierarchy. See *Understanding and Using NetInfo*, available at www.apple.com/macosx/server/, for complete information on how to set up Authentication Manager.

Setting Up Windows Services for the First Time

All you need to do to set up Windows services is to start it. The default settings will work well in most cases, but you'll probably want to take a look at the settings and change anything that isn't appropriate for your network. For a description of the settings you can make, see "Windows Services Settings," next.

Follow the steps below to set up Windows services for the first time. If you need more detailed instructions for any of these steps, see the onscreen help.

Step 1: Configure Windows services

In Server Admin, click the File & Print tab, then click Windows and choose Configure Windows Services. Click each of the four tabs in the Windows Services Settings window to see the settings and change any that you need to. For a description of the available settings, see "Windows Services Settings," next.

Step 2: Start Windows services

Click Windows and choose Start Windows Services. A globe appears on the service icon when the service is turned on.

Step 3: Check client configurations

After you set up Windows services, you should make sure your Windows client computers are configured properly to connect over TCP/IP. If you need more information about this, consult your Windows networking documentation.

Windows Services Settings

To access Windows services settings, click the File & Print tab, then click Windows and choose Configure Windows Services. Click each of the four tabs to see the settings for that pane. The settings available in each pane are described in the following sections.

General Settings

You use the General pane to set identifying information about your Windows server, and to enable automatic startup. To access the General pane, click Windows and choose Configure Windows Services.



Server Name

Type the server name you want users to see when they connect. The default name is the NetBIOS name of the Windows file server. The name should contain no more than 15 characters, and no special characters or punctuation.

If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.apple.com," give your server the name "server."

Workgroup

Type the name of the workgroup that you want users to see in the Network Neighborhood window. If you have Windows domains on your subnet, use one of them as the workgroup name to make it easier for clients to communicate across subnets. Otherwise, consult your Windows network administrator for the correct group name. The workgroup name cannot exceed 15 characters.

Description

Type a description, no longer than 43 characters, that is meaningful to you or your users. This description appears in the Network Neighborhood window on client computers, and it is optional.

Code Page

Choose the code page for the language client computers will use.

Start Windows Services on system startup

Select this option if you want to ensure that the server is restarted after a power failure or other unexpected event. In most cases it's best to select this option.

Access Settings

You use the Access pane to allow guest access and set the maximum client connections. To find the Access pane, click Windows and choose Configure Windows Services, then click the Access tab.



Allow Guest access

Select this option only if you want to allow people who are not registered users to use Windows file sharing. This is a convenient way to provide occasional users with access to files and other items for which the appropriate privileges have been set.

Maximum client connections

Type the maximum number of concurrent connections you want to allow. This number is limited by the type of software license you own. If you are using your server to provide a number of services, you can improve performance by setting the maximum connections to a value lower than the license allowed by your server.

Logging Settings

You use the Logging pane to choose the level of detail you want in your log. To access the Logging pane, click Windows and choose Configure Windows Services, then click the Logging tab.



Detail Level

Choose the level of detail you want logged. The more detailed the logging, the larger the log file. The table below shows the level of detail you'll get for each option.

Events logged	None	Minimal	Verbose
Starting and stopping the server	No	Yes	Yes
When users try and fail to log in	No	Yes	Yes
Warnings and errors	Yes	Yes	Yes
When browser name registration occurs	No	Yes	Yes
Access events (each time a file is opened, modified, read, and so on)	No	No	Yes

Neighborhood Settings

You use the Neighborhood pane to set up name resolution and enable browsing across subnets. To access the Neighborhood pane, click Windows and choose Configure Windows Services, then click the Neighborhood tab.



WINS

Choose whether you want to register with a WINS server, either locally or externally. Your choices are

- *Off*: Your server will not register itself with any external WINS server or local name resolution server.
- *Enable WINS server*: The file server will provide local name resolution services. This allows clients across multiple subnets to perform name/address resolution.
- *Register with WINS server*: Choose this setting if your Windows clients and Windows server are not all on the same subnet, and your network has a WINS server. Then enter the IP address or DNS name of the WINS server.

Workgroup/Domain

Choose whether to enable domain browsing services. Your choices are

- *Master Browser*: Provides browsing and discovery of servers in a single subnet
- *Domain Master Browser*: Provides browsing and discovery of servers across subnets

Solving Problems With Windows Services

If users can't see the Windows server in the Network Neighborhood:

- Make sure users' computers are properly configured for TCP/IP and have the appropriate Windows networking software installed.
- Enable guest access for Windows users.
- Go to the DOS prompt on the client computer and type "ping [IP address]," where "IP address" is your server's address. If the ping fails, then there is a TCP/IP problem.
- If users' computers are on a different subnet from the server, you need to have a WINS server on your network.

Note: If Windows computers are properly configured for networking and connected to the network, client users can connect to the file server even if they can't see the server icon in the Network Neighborhood window. For instructions, see "Connecting to the Windows server without the Network Neighborhood" in Server Admin Help.

If a Windows user can't log in:

- Ensure that Authentication Manager is enabled for the NetInfo domain the user's record resides in, and all other NetInfo domains in the NetInfo hierarchy.
- Reset the user's password and try again.
- Enable Windows users to be authenticated using cleartext password validation.

Windows Services Specifications

Maximum number of connected users, depending on your license agreement	1000
Maximum volume size	2 terabytes
TCP port number	139
UDP port numbers	137, 138
Log file location	/Library/Logs in the WindowsFileServices folder

Network File System (NFS) Service

Apple file service, Windows file sharing, and FTP service allow users to connect to shared items based on a user name and password. NFS is different—it allows access to information based on the computer’s IP address. This means that a particular client computer will have access to certain share points regardless of who is using it. Whenever the computer is started up, some volumes or folders are automatically mounted or made available, and anyone who uses the computer has access to them.

In NFS, you don’t “share” items, you “export” them. Exporting is like publishing a share point to a specific destination. You use the NFS module of Server Admin to configure and manage NFS service. You also use the Sharing module of Server Admin to set privileges and access levels for the share points or folders you want to export.

Who Should Use NFS Service?

NFS, unlike the other file services in Mac OS X Server, doesn’t provide a high degree of precision in setting up access levels. You can export a shared item to a set of client computers or to “World.” Be aware that exporting an NFS volume to World means that anyone who can access your server (including anonymous FTP users) can also access that volume.

You should probably only use NFS service if you are on a local area network (LAN) with trusted client computers, or if you are in an environment that can’t use Apple file sharing or Windows file sharing. If you have Internet access and plan to export to World, your server should be behind a firewall.

Before You Set Up NFS Service

Be sure to consider the security implications of exporting in NFS. NFS was created for a secure networking environment, and trusts the client computers and the people who administer the clients.

With NFS, it’s possible for a user to take over ownership of another person’s files. For example, if a file on the server is owned by a user with user ID 1234, and you export a folder that contains that file, someone on a remote computer can create a local user on the remote computer, give it a user ID of 1234, mount that folder, and have the same access to the folder’s contents as the file’s original owner.

You can take some steps to prevent this by creating unique user IDs, and by safeguarding user information.

Setting Up NFS for the First Time

Step 1: Configure NFS service

In Server Admin, click the File & Print tab, then click NFS and choose Configure NFS. Set the maximum number of daemons (server processes that handle client requests) that you want to allow at one time, and then choose whether you want to use TCP or UDP to send data to clients. For more information about these options, see “NFS Service Settings,” next.

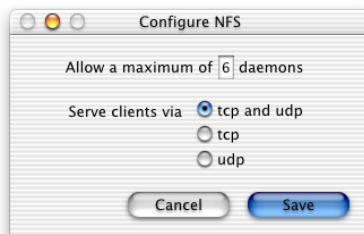
Step 2: Export a folder and start NFS service

When you first set up NFS, you should share at least one folder. To do this, click the General tab in Server Admin, click Sharing, then choose Set Sharing Attributes. Select the folder you want to share and click Choose. Choose General, Automount, and NFS Access Control from the pop-up menu and make the settings you want. For information on the options you can set, see “NFS Access Control Settings” on page 102.

You don’t need to start or stop NFS service; when you define a share point to export, the service starts automatically. When you delete all exports, the service stops. You can tell if NFS service is running by looking for the globe on the NFS icon in Server Admin.

NFS Service Settings

You configure NFS service using the Configure NFS window. To access this window, click the File & Print tab, then click NFS and choose Configure NFS.



Allow a maximum of _ daemons

Enter the maximum number of nfsd daemons you want to allow at one time. An nfsd daemon is a server process that runs continuously behind the scenes and processes reading and writing to mounted share points. The more daemons that are available, the more concurrent clients can be served. For Mac OS X Server, set the maximum number of daemons on your server to a value between four and six.

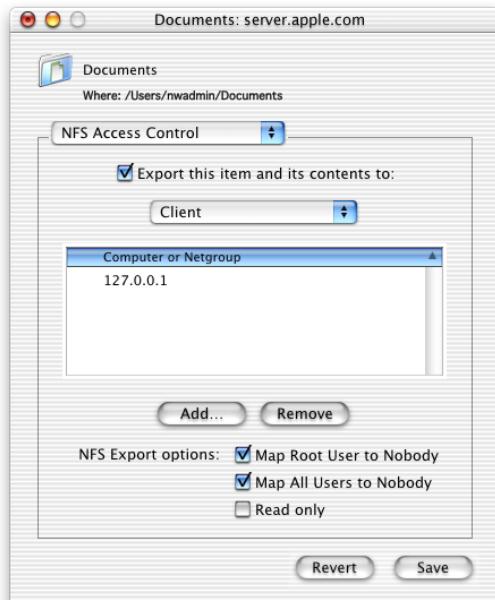
Serve clients via

Choose how you want to serve data to your client computers.

- **TCP:** Transmission Control Protocol (TCP) separates data into packets (small bits of data sent over the network using IP) and uses error correction to make sure information is transmitted properly.
- **UDP:** User Datagram Protocol (UDP) doesn't break data into packets, so it uses fewer system resources. It's more scalable than TCP, and a good choice for a heavily used server.
- **TCP and UDP:** You should select both TCP and UDP unless you have a specific performance concern. TCP provides better performance for clients, and UDP puts a smaller load on the server.

NFS Access Control Settings

You use the NFS Access Control pane to create exports and set access privileges for them. To find the NFS Access Control pane, click the General tab in Server Admin. Click Sharing and choose Show Disks & Share Points. Select a shared item and click Privileges, then choose NFS Access Control from the pop-up menu below the shared item name.



Export this item and its contents to

Select this option to export the item and make it available to users. Choose whom you want to be able to use this information. You can choose Client or World from the pop-up menu. If you choose to export to World, there is a potential security risk.

The default configuration for NFS exports to the client address 127.0.0.1, which is a loopback to the server computer. This prevents you from inadvertently exporting a folder to World.

Add and Remove

Click Add to designate clients who can receive this export. Type the IP address or host name in the text box that appears to add them to the Computer or Netgroup list. Choose an IP address from the list and click Remove to delete the client from the export list.

NFS Export options

Map Root User to Nobody: Choose this option if you want users identified as “root” on the remote client system to have only minimal privileges to read, write, and execute commands.

Map All Users to Nobody: Choose this option if you want all users to have minimal privileges to read, write, and execute.

Read only: Choose this option if you don’t want client users to be able to modify the contents of the shared item in any way. This overrides any other privileges set for the shared item. For example, if you allow the “Everybody” category Read & Write privileges for the item in Apple file service, you can also define it as an NFS export to “World” with “Read only” privileges.

File Transfer Protocol (FTP) Service

FTP allows computers to transfer files over the Internet. Clients using any operating system that supports FTP can connect to your file server and download files, depending on the permissions you set. Most Internet browsers and a number of freeware applications can be used to access your FTP server.

Before You Set Up FTP Service

Consider the type of information you need to share and who your clients are when determining whether or not to offer FTP service. FTP works well when you want to transfer large files such as applications and databases. In addition, if you want to allow guest (anonymous) users to download files, FTP is a secure way to provide this service.

Restrictions on Anonymous FTP Users (Guests)

Enabling anonymous FTP poses a security risk to your server and data because you open your server to users that you do not know. The access privileges you set for the files and folders on your server are the most important way you can keep information secure.

Anonymous FTP users are only allowed to upload files into a share point named “uploads.” If the uploads share point doesn’t exist, anonymous users will not be able to upload files at all.

To ensure the security of your FTP server, by default anonymous users cannot

- delete files
- rename files
- overwrite files
- change permissions of files

Setting Up FTP Service for the First Time

Step 1: Create share points

You use the Sharing module of Server Admin to set up the share points that you want to make available through FTP. For instructions on creating share points, read “Setting Up Sharing for the First Time” on page 76.

Step 2: Configure FTP service

Most of the configuration for FTP service happens behind the scenes when you turn the service on. You can, however, modify a few settings, such as allowing guest access and setting the maximum number of guest and registered users who can be logged in at the same time.

To access FTP service settings, click the File & Print tab in Server Admin, then click FTP and choose Configure FTP. For a description of the available settings, see the next section, “FTP Service Settings.”

Step 3: Start FTP service

Click FTP and choose Start FTP Service. A globe appears on the service icon when the service is turned on.

Step 4: Set up anonymous FTP service (optional)

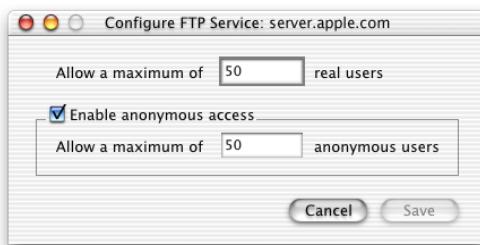
If you enable guest access, anonymous users can log in using the name “ftp” or “anonymous.” They do not need a password to log in, but they will be prompted to enter their email address.

To enable guest access, click FTP and choose Configure FTP. Then select “Anonymous access enabled.”

If you want guest users to be able to upload files, create a folder named “uploads” and assign appropriate access privileges to it using the Sharing module of Server Admin.

FTP Service Settings

To access FTP service settings, click FTP in Server Admin and choose Configure FTP.



Allow a maximum of _ real users

Enter a value in the field to set the maximum number of registered users who can connect to your server at the same time. Real users are users who have been added in the Users & Groups module of Server Admin.

Enable anonymous access

Select this checkbox to allow anonymous users to connect to the server and transfer files. You should review the privileges assigned to your share points carefully to make sure there are no security holes. For more information about keeping your information secure, read Chapter 4, “Sharing.”

Allow a maximum of _ anonymous users

Enter a value in the field to set the maximum number of anonymous users who can connect to your server at the same time.

FTP Service Strategies and Tips

Displaying Messages to Users

FTP service in Mac OS X Server allows you to create certain messages that you can send to real users and to anonymous FTP users when they log in to your server. Some FTP clients may not display the message in an obvious place, or they may not display it at all. For example, the FTP client Fetch displays a banner message in the “RemoteHostname Messages” window.

Banner Message

When users first try to connect to the FTP server, they receive a message before they see the login prompt. You can modify this message using a text editor such asTextEdit. Look for the file “banner.txt” located in this directory:

/Library/FTPServer/Messages/banner.txt

Welcome Message

Users receive a welcome message when they successfully log in to the FTP server. You can modify this message using a text editor such asTextEdit. Look for the file “welcome.txt” in this directory:

/Library/FTPServer/Messages/welcome.txt

Message

When a user encounters a directory that contains a file named “message.txt,” the file content is displayed as a message. The user only sees the message the first time he or she connects to the directory during that FTP session. You can use the message to notify users of important information, or changes users need to be aware of.

README Message

You can also place a file called “README” in a directory. When users encounter a directory that contains a README file, they receive a message letting them know that the file exists, and when it was last updated. Users can choose whether or not to open and read the file.

Inside FTP Service

FTP service in Mac OS X Server is based on the source code for Washington University’s FTP server, known as “wu-FTPd.” However, modifications have been made to the original source code to deliver a better user experience. Some of these differences are described in this section.

Secure FTP Environment

Most FTP servers provide a restricted directory environment that confines FTP users to a specific area within a server. Users can only see volumes in this area, so the server is kept quite secure. However, users cannot access volumes mounted outside this restricted area. Symbolic links and aliases don't reach across the boundaries set within the server.

FTP service in Mac OS X Server uses a new approach that still provides a secure FTP environment. FTP users can access volumes mounted anywhere on the server, as long as the permissions set for the volumes allow it. FTP users will see any share points that you set up in the Sharing module of Server Admin. You control the security of your data by setting appropriate access privileges for your share points. For more information about creating share points, see Chapter 4, “Sharing.”

Home Directories for Real Users

Standard FTP servers assume that “real users” (those that use registered user names and passwords to log in) are trusted to have full access to the server. This model is no longer as relevant as it was in the early days of the Internet—now you may have thousands of registered users who are not known to you. Instead, FTP service in Mac OS X Server always places both real and anonymous users into the restricted FTP environment. However, it connects real users to their own home directories if the directories are available within the restricted environment. So, for example, if a user's home directory is contained within a share point, and access privileges allow the user to access his or her home directory, the user is placed into the home directory after logging in.

An important point to remember is that both real and anonymous users can see home directories in a share point. They can't access these directories, however, unless the appropriate privileges have been set.

Important If you have real users who don't have home directories, or if their home directories are not located in a share point to which they have access, they will be put at the root level of the restricted FTP environment.

On-the-Fly File Conversion

FTP service in Mac OS X Server allows users to request compressed or decompressed versions of information on the server. A filename suffix such as “.Z” or “.gz” indicates that the file is compressed. If a user requests a file called “Hamlet.txt” and the server only has a file named “Hamlet.txt.Z,” it knows that the user wants the decompressed version, and delivers it to the user in that format.

In addition to standard file compression formats, Mac OS X Server has the ability to read files from either HFS, or non-HFS volumes, and convert them to MacBinary (.bin) format. This is one of the most commonly used file compression formats for the Macintosh operating system. The table below shows common file extensions and the type of compression they designate.

File extension	What it means
.Z	UNIX Compress
.bin	MacBinary Encoding
.tar	UNIX tar archive
.tZ	UNIX Compressed tar archive
.tar.Z	UNIX Compressed tar archive
.crc	UNIX checksum file

Solving Problems With FTP Service

If anonymous users can't connect:

- Verify that guest access is turned on.
- See if the maximum number of anonymous user connections has been reached. To do this, click the Networking tab in Server Admin, click FTP, then choose Configure FTP.

If clients can't connect to the FTP server:

See if the client is using FTP passive mode, and turn it off. Passive mode causes the FTP server to open a connection on a dynamically determined port to the client, which could conflict with port filters set up in IP filter service.

If FTP connections are refused:

- Verify that the user is entering the correct DNS name or IP address for the server.
- Make sure FTP service is turned on.
- Make sure the user has appropriate access privileges to the shared volume.
- See if the maximum number of connections has been reached. To do this, click the Networking tab in Server Admin, click FTP, then choose Configure FTP.
- Verify that the user's computer is configured correctly for TCP/IP. If there doesn't appear to be a problem with the TCP/IP settings, use a "pinging" utility to check network connections.
- See if there is a DNS problem by trying to connect using the IP address of the FTP server instead of its DNS name. If the connection works with the IP address, there may be a problem with the DNS server.

- Verify that the user is correctly entering his or her short name and typing the correct password. User names and passwords with special characters or double-byte characters will not work. To find the user's short name, double-click the user's name in the Users & Groups List.
- See if there are any problems with directory services, and if the directory services server is operating and connected to the network. For help with directory services, see Chapter 2, "Directory Services."
- Verify that IP filter service is configured to allow access to the appropriate ports. If clients still can't connect, see if the client is using FTP passive mode and turn it off. Passive mode causes the FTP server to open a connection to the client on a dynamically determined port, which could conflict with port filters set up in IP filter service. For a list of common TCP and UDP ports, see "Ports Used by Mac OS X Computers" on page 301.

FTP Service Specifications

Maximum number of connected users (the default setting is 50 for real users and 50 for anonymous users)	1000
FTP port number	21
Number of failed login attempts before user is disconnected	3

Where to Find More Information About File Services

For more information about the protocols used in Mac OS X Server file services, see these resources:

- *Apple Filing Protocol (AFP)*: www.apple.com/developer/
- *Server Message Block (SMB) protocol (for Windows file services)*: www.samba.org
- *FTP*: You can find a Request for Comments (RFC) document about FTP at the following Web site: www.faqs.org/rfcs/rfc959.html
RFC documents provide an overview of a protocol or service that can be helpful for novice administrators, as well as more detailed technical information for experts. You can search for RFC documents by number at this Web site: www.faqs.org/rfcs
- To obtain the UNIX manual pages for FTP, open the Terminal application in Mac OS X. At the prompt, type "man ftp" and press the Return key.
- *NFS*: To obtain the UNIX manual pages for NFS, open the Terminal application in Mac OS X. At the prompt, type "man nfs" and press the Return key.

Print Service

What Is Print Service?

Print service lets you share PostScript-compatible printers among client users who submit print jobs using the industry-standard LPR printing protocol or the Windows Server Message Block (SMB) protocol.

Several applications help you administer print service:

- Use the Print Center application to select printers you want to make available for sharing.
- Use the Print module of Mac OS X Server to configure general print service settings, to set up how print queues are shared, and to manage print jobs submitted to shared printers.
- Use the Log Viewer in Server Admin to view information related to print job accounting.

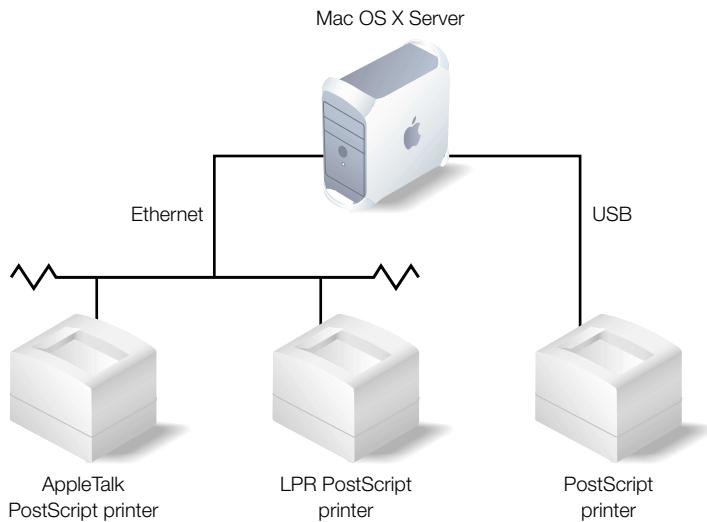
This chapter first summarizes each of these activities, then describes how to set up and troubleshoot print service.

Connecting Printers to the Server

You use the Mac OS X Print Center application (located in Applications/Utilities) to “add” printers to the server, creating a print queue for each printer you want to share. You can share any PostScript-compatible printer that you can add using Print Center.

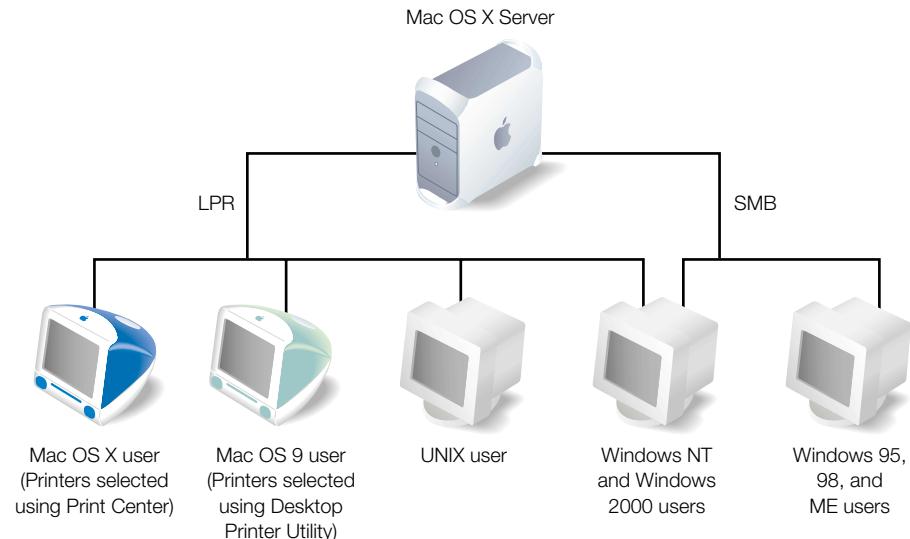
You can also share any PostScript-compatible printer that’s directly connected to your server. You do not need to add a queue for it; the queue is created automatically when you open Print Center.

Shared PostScript-compatible printers with network interfaces can be connected to the network using AppleTalk or the industry-standard LPR protocol (based on TCP/IP). Directly connected printers use a Universal Serial Bus (USB) connection:



Sharing Queues Over the Network

Shared printers can be used over the network by users who submit print jobs using LPR or SMB protocols:



Macintosh, UNIX, and some Windows computers (such as Windows NT and Windows 2000) all support LPR without installing additional software. All Windows computers—including Windows 95, Windows 98, and Windows Millennium Edition (ME) computers—support SMB.

Note: Third-party LPR drivers are available for Windows computers that do not have built-in LPR support.

Managing Print Queues and Their Jobs

When users submit print jobs to a shared printer, the jobs are automatically sent to the printer's queue, where they are held until the printer becomes available or criteria you set up have been met. For example, using the Server Admin Print module, you can

- Set the priority of print jobs in a queue. Jobs with a priority of Urgent are printed before those with a priority of Normal or Low.
- Schedule the printing of a job for a particular time of day. For example, you can schedule time-consuming jobs to start automatically when printers are not in high demand, such as late at night or early in the day.
- Place a job on hold indefinitely. You may, for example, need to verify that a user hasn't exceeded a printing limit or budget before releasing a particular job for printing.

Monitoring Print Jobs

The Print module of Server Admin has a Print Monitor that provides an up-to-the-minute snapshot of your printers and their jobs. You can see at a glance whether a particular printer has a large number of jobs waiting to be printed and whether a printer needs your attention.

The Print module also has a Queue Monitor, which lets you view job details for a print queue. The user who submitted the job, the number of pages, and the priority are displayed for each job, and you can hold, delete, or prioritize queued jobs.

You can also track printing activities by viewing the print logs using Server Admin's Log Viewer. A print service log records such events as when print service was started and stopped and when a print queue was put on hold. Separate logs for each print queue record individual print jobs, including such information as which users submitted jobs for particular printers and the size of the jobs.

Before You Set Up Print Service

Before setting up print service, determine whether a particular printer will be used by

- users who submit print jobs using the LPR protocol
- users who submit print jobs using the SMB protocol

Setting Up Print Service for the First Time

To set up print service, you use Print Center to add the printers whose queues you want to manage and share, and the Server Admin Print module to configure each queue. After adding printers, do not use Print Center for queue or job management; use the Server Admin Print module instead.

Follow these steps to set up print service:

Step 1: Add printers

Use Print Center to add each non-USB printer you want to manage on your Mac OS X Server. The onscreen help for Print Center tells you how. A print queue is automatically defined for every printer you add.

Step 2: Configure print service

Use the Print module of Server Admin to configure print service. See “General Print Service Settings” on page 115 for an explanation of the available settings.

Step 3: Configure print queues

Use the Print module of Server Admin to configure the queue for each printer you added. See “Print Queue Settings” on page 116 for an explanation of print queue settings.

Step 4: Start print service

If print service is not already running, click Print and choose Start Print Service. You can configure print service to start automatically when the Mac OS X Server starts up. See “General Print Service Settings” on page 115 for instructions.

Step 5: Enable Windows services (optional)

To enable printing by Windows users who submit jobs using SMB, make sure Windows services are running and that one or more print queues are available for SMB use. See “Windows Services” on page 93 for more information about Windows services. See “Print Queue Settings” on page 116 for a description of how to share a print queue for SMB users and “General Print Service Settings” on page 115 for how to automatically enable SMB printing for any new queue that is created.

Step 6: Set up printing from client computers

See the onscreen help for print service for instructions on setting up printing to the queues you configured in step 3 from Mac OS 8, Mac OS 9, and Mac OS X computers.

Print Service Settings

To access print service settings, click the File & Print tab in Server Admin, then click Print and choose the appropriate command.

General Print Service Settings

To access settings that control general print service behavior, click Print and choose Configure Print Service.



Start print service at system startup

Select this option if you want print service to start automatically when the server starts up.

Automatically share new queues for Windows printing

Select this option if you want Windows users who print using the SMB protocol to be able to automatically use new print queues that you create using Print Center. If you select this option, ensure that Windows services are running. See “Windows Services” on page 93 for more information about Windows services.

Default Queue for LPR

Choose the queue you want to use when an LPR print job without a queue name arrives. A job has no queue name if a user submits it by using your server’s domain name or IP address, but no printer name. Using a default queue simplifies the setup for printing from client computers, since no queue name needs to be specified.

Server log

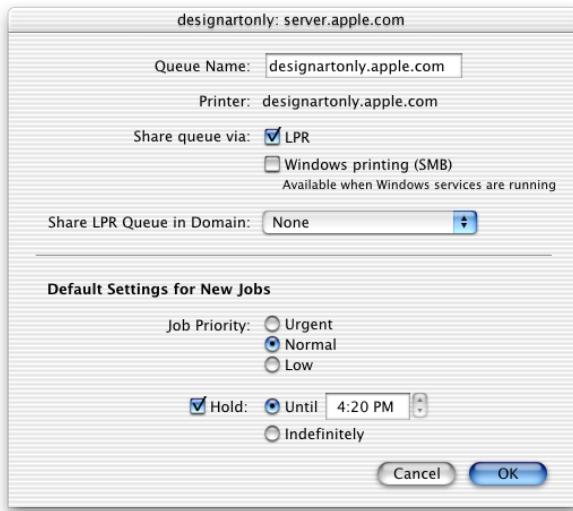
Select this option and enter a number of days to specify how often you want to archive the print service log and start a new log.

Queue logs

Select this option and enter a number of days to specify how often you want to archive each print queue log and start a new one.

Print Queue Settings

To manage how a queue is shared and to specify when new jobs in the queue are printed by default, select the queue name in the Print Monitor window, then click the Edit button. (To open the Print Monitor window, click Print in the File & Print tab and choose Show Print Monitor.)



Queue Name

When you add a printer in Print Center, the name of the queue created for it is the same as the printer name. You can change the queue name if you like (for example, if you want users to see a different name for the queue) by entering a name in the Queue Name field. Entering a queue name does not change the Print Center queue name.

You'll probably need to change the queue name if users who print to your queues have restrictions on printer names they can use. For example, some LPR clients do not support names that contain spaces, and some Windows clients restrict names to 12 characters.

Printer

This is the Print Center queue name.

Share queue via

Select LPR to make the queue available to users who submit jobs using the LPR protocol. By default, LPR is selected for all new print queues.

Select “Windows printing (SMB)” to make the queue available to Windows users who submit jobs using SMB. If you select this option, ensure that Windows services are running. See “Windows Services” on page 93 for more information about Windows services. See “General Print Service Settings” on page 115 to learn how to automatically enable SMB printing for any new queue.

These checkboxes are disabled for printers that are not PostScript-compatible.

Share LPR Queue in Domain

If you add a print queue to a shared NetInfo domain, users of Mac OS X computers configured to access the domain can print to the queue after choosing it from the Directory Services list in Print Center.

To add a print queue to a shared domain, choose the shared domain from the pop-up menu, then enter the user name and password for the administrator of the server on which the domain resides. Choose None if you don’t want to add the queue to a shared NetInfo domain.

After sharing an LPR queue in a NetInfo domain, do *not* use Print Center on the server to add the queue by choosing it from the Directory Services list.

Job Priority

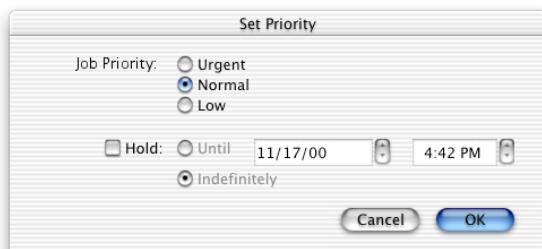
Select the priority you want assigned by default to new print jobs in this queue. Jobs are printed in priority order: Urgent jobs are printed first, then Normal jobs, and finally Low jobs. You can override the default priority for individual jobs by using the print job settings, described in “Print Job Settings,” below.

Hold

Select Hold to postpone printing all new jobs that arrive in the queue. You can specify a time of day to print the jobs, or you can postpone printing indefinitely.

Print Job Settings

To control when a specific job prints, select its name in the Queue Monitor window, then click the Priority button. (To open the Queue Monitor, select a queue in the Print Monitor window and click Show Queue Monitor.)



Job Priority

Select the priority you want to assign to the job. Urgent jobs are printed first, then Normal jobs, and finally Low jobs. The job is printed after any older jobs in the queue with the same priority.

Hold

Select Hold to postpone printing the job. You can specify a date and time to print the job or postpone printing it indefinitely. To take a job off hold, deselect Hold or click Release in the Queue Monitor window; the job prints after any other jobs in the queue that are not on hold and that have the same priority. Jobs that are not on hold only print if their queue is not on hold.

Solving Problems With Print Service

Try these suggestions to solve or avoid printing problems.

If print service doesn't start:

- If you expect print service to start automatically when the server starts up, make sure the “Start print service at system startup” checkbox is selected in the Configure Print Service window.
- To verify that the server’s serial number is entered correctly and has not expired, click the General tab, click Server Info, and choose Show Server Info.
- To review the print service log for additional information, click the General tab, click Log Viewer, and choose Print Service. In the Log Viewer window, choose Server Log.

If users can't print:

- Check to see that print service is running.
- Make sure that the queue users are printing to exists by opening the Print Monitor window. On Mac OS 8 or Mac OS 9 computers, use the Desktop Printer Utility to make sure the printer setup is correct.
- Verify that the queue users are printing to is shared correctly. SMB is for Windows users only. LPR is a standard protocol that users on (some) Windows computers, as well as Macintosh, UNIX, and other computers, can use for printing.
- Verify that Mac OS 8 and Mac OS 9 clients have TCP/IP set up correctly.
- If Windows NT 4.x clients can't print to the server, make sure that the queue name is not the TCP/IP address of the printer or server. Use the DNS host name instead of the printer or server address or, if there is none, enter a queue name containing only letters and numbers.

If print jobs are accepted without error messages, but don't print:

- Check the Print Monitor window to make sure that the queue is not on hold.
- Ensure that the printer is connected to the server or to the network to which the server is connected.
- Make sure the printer is turned on and that there are no problems with the printer itself (out of paper, paper jams, and so on).
- Review the print logs for additional information. Click the General tab, click Log Viewer, and choose Print Service. In the Log Viewer window, choose Server Log to review the general print service log, or choose a queue name to review the log for a particular printer.

Web Service

What Is Web Service?

Web service in Mac OS X Server offers an integrated Internet server solution. Web service is easy to set up and manage, so you don't need to be an experienced Web administrator to set up multiple Web sites and configure and monitor your Web server.

Web service in Mac OS X Server is based on Apache, an open source HTTP Web server. AppleShare IP and new Web administrators can use Server Admin to administer Web service without knowing anything about advanced settings or configuration files. Web administrators proficient with Apache can choose to administer Web service using Apache's advanced features.

In addition, Web service in Mac OS X Server includes a high performance, front-end cache that improves performance for Web sites that use static HTML pages. With this cache, static data doesn't need to be accessed by the server each time it is requested.

Web service also includes support for Web-based Distributed Authoring and Versioning, known as WebDAV. With WebDAV capability, your client users can check out Web pages, make changes, then check them back in while the site is running. In addition, the WebDAV command set is rich enough that client computers with Mac OS X installed can use a WebDAV-enabled Web server as if it were a file server.

Before You Set Up Web Service

This section provides information you'll need to know before you set up Web service for the first time. You should read this section even if you are an experienced Web administrator, as some features and behaviors may be different from what you expect.

Configuring Web Service

You can use Server Admin to set up and configure the most frequently used features of Web service. If you are an experienced Apache administrator and need to work with features of the Apache Web server that aren't included in Server Admin, you can modify the appropriate configuration files. However, Apple does not provide technical support for modifying Apache configuration files. If you choose to modify a file, be sure to make a backup copy first. Then you can revert to the copy should you have problems.

For more information about Apache modules, see the Apache Software Foundation Web site at www.apache.org

Providing Secure Transactions

If you want to provide secure transactions on your server, you should set up Secure Sockets Layer (SSL) protection. SSL lets you send encrypted, authenticated information across the Internet. If you want to allow credit card transactions through your Web site, for example, you can use SSL to protect the information that's passed to and from your site.

For instructions on how to set up secure transactions, see “Setting Up Secure Sockets Layer (SSL) Service” on page 142.

Setting Up Web Sites

Before you can host a Web site, you must

- register your domain name with a domain name authority
- create a folder for your Web site on the server
- create a default page in the folder for users to see when they connect
- configure DNS service properly if you are connected to the Internet (sites located on an intranet don't need DNS)

When you are ready to publish, or enable, your site, you can do this using Server Admin. The Sites pane in the Configure Web Service window lets you add a new site and select a variety of settings for each site you host. You should read the information about site settings that begins on page 130. You can also find information about some of the tasks involved in setting up a site in Server Admin Help.

Hosting More Than One Web Site

You can host more than one Web site simultaneously on your Web server. Depending on how you configure your sites, they may have the same domain name, IP address, or port.

However, the combination of domain name, IP address, and port must be unique for each site. Your domain names must be registered with the domain name authority (InterNIC). Otherwise, the Web site associated with the domain won't be visible on the Internet. (There is a fee for each additional name you register.)

If you configure Web sites using multiple domain names and one IP address, older browsers that do not support HTTP 1.1 or later (that don't include the "Host" request header), will not be able to access your sites. If you think that this could be a problem for your users, you'll need to configure your sites with one domain name per IP address.

Understanding WebDAV Security

WebDAV lets users update files in a Web site while the site is running. When WebDAV is enabled, the Web server must have write access to the files and folders within the site users are updating. This has significant security implications when other services are running on the server, because individuals responsible for one site may be able to modify other sites.

You can avoid this problem by carefully setting access privileges for the site files using the Sharing module of Server Admin. Mac OS X Server adds a group named "www," which contains the Apache processes, to the Users & Groups List. You need to give the www group Read & Write access to files within the Web site. You'll also need to assign Read & Write access to the Web site administrator (owner), and None to Everyone.

If you are concerned about Web site security, you may choose to leave WebDAV disabled and use Apple file service or FTP service to modify the contents of a Web site instead. For more information about WebDAV privileges, see "Understanding WebDAV Realms and Privileges" on page 149.

Setting Up Web Service for the First Time

Follow the steps below to set up Web service for the first time. If you need more information to perform any of these tasks, see Web Service Help.

Step 1: Set up the Documents folder

When your server software is installed, a folder named Documents is set up automatically. Put any items you want to make available through a Web site in the Documents folder. You can create folders within the Documents folder to organize the information. The folder is located in this directory:

/Library/WebServer/Documents

In addition, each registered user has a Sites folder in the user's own home directory. Any graphics or html pages stored here will be served from this URL:

<http://server.example.com/~username/>

Step 2: Create a default page

Whenever users connect to your Web site, they see the default page. When you first install the software, the file “index.html” in the Documents folder is the default page. You’ll need to replace this file with the first page of your Web site and name it “index.html.” If you want to call the file something else, make sure you change the default document name in the General pane of the site settings window.

For more information about Web site settings, see “Web Site Settings” on page 130.

Step 3: Assign privileges for your Web site

The Apache process running on the server must have access to the Web site’s files and folders. To allow this access, Mac OS X Server installs a group named “www” made up of the Apache processes in the server’s Users & Groups database. You need to give the www group Read Only access to files within your Web site so that it can transfer those files to browsers when users connect to the site. For information about assigning privileges, see Chapter 4, “Sharing.”

Step 4: Configure Web service

The default configuration works for most Web servers that host a single Web site. You can configure all the basic features of Web service and Web sites using Server Admin. For more advanced configuration options, see “Advanced Apache Configuration” on page 147.

To host user Web sites, you must configure at least one Web site. If you want your configuration settings to apply to all user Web sites on your server, you must set the default site to /Users.

To access the configuration settings, click Web and choose Configure Web Service. Choose the settings you want for your server and your Web site. For information about these settings, see “Web Service Settings” on page 125.

Step 5: Start Web service

Click Web and choose Start Web Service. When the service is running, you see a globe on the Web icon.

Important Always use Server Admin to start and stop the Web server. If you start the Web server from the command line, Server Admin won’t be able to stop it, and won’t know that the Web server is running.

Step 6: Connect to your Web site

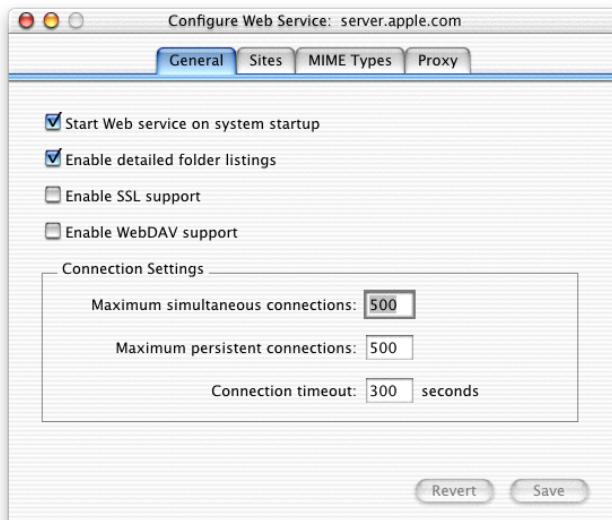
To make sure the Web site is working properly, open your browser and try to connect to your Web site over the Internet. If your site isn’t working correctly, see “Solving Problems With Web Service” on page 149.

Web Service Settings

The Configure Web Service window lets you set and modify all the options for your Web server and Web sites. To access the Configure Web Service window, click Web and choose Configure Web Service. Click one of the five tabs to see the settings in that pane. The settings available in each pane are described in the following sections.

General Settings for Web Service

Use the General pane of the Configure Web Service window to set general options for the server, such as automatic startup.



Start Web service on system startup

Select this option if you want Web service to start whenever the server starts up. In most cases it's best to turn on this option. This ensures that if the server is restarted after a power failure or other unexpected event, Web service will be available.

Enable detailed folder listings

Select this option if you want users to see a formatted list of the contents of a Web site's folder. When users connect to the URL for a site, normally a default Web page is displayed (such as index.html). If a default Web page doesn't exist, and folder indexing is enabled for the Web site, users will see a list of the folder contents. For information on enabling folder indexing for a site, see "General Settings for Web Sites" on page 131.

Enable SSL Support

Select this option if you want to provide secure connections for your Web sites. If you enable SSL, you also need to change the port number to 443 for each site.

Before you enable SSL, you must obtain a certificate file from a certificate provider and set up SSL service. For more information, see “Setting Up Secure Sockets Layer (SSL) Service” on page 142.

Enable WebDAV support

Select this option if you want your users to be able to use Web-based Distributed Authoring and Versioning (WebDAV). If you enable WebDAV, you also need to set up “realms” for each Web site to control which users have the ability to make changes to the site. For more information on using WebDAV, see “Understanding WebDAV Realms and Privileges” on page 149.

Maximum simultaneous connections

Type the maximum number of connections any one Web site on your server can accept simultaneously. The default maximum value is 500. When the server reaches the maximum number of simultaneous connections, new connection requests receive a message that the server is busy.

Maximum persistent connections

Type the maximum number of connection requests you want to allow client computers to make on a single connection. Allowing persistent connections lets the server use a single connection to complete several transactions, which improves server performance. Set the number to zero if you don’t want to limit the number of requests allowed per connection. However, the default setting of 500 provides better performance.

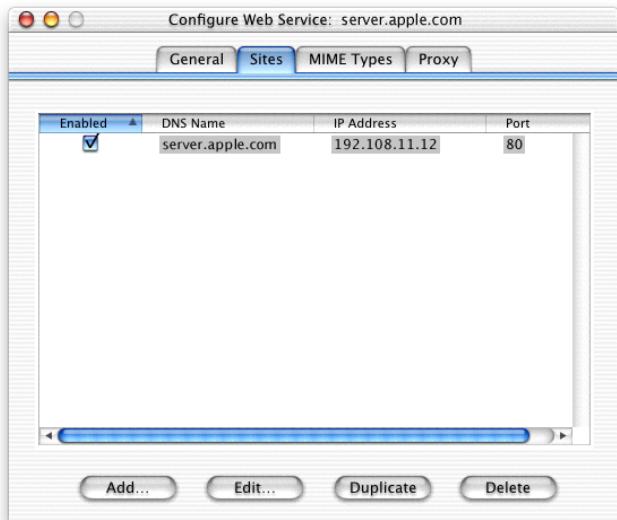
Note: You need to disable the performance cache to use this option.

Connection timeout

Type the number of seconds that can pass between requests before the session is disconnected by the Web server. You need to disable the performance cache to use this option.

Sites Settings for Web Service

The Sites pane lists your Web sites and provides some basic information about each one. You use the Sites pane to add new sites or change settings for existing sites. To access the Sites pane, click Web and choose Configure Web Service, then click the Sites tab.



Enabled

Select this checkbox to turn a site on or off. By default, this box is selected whenever you create a new site. Turning a site off preserves its settings but ignores requests directed to it.

Add and Duplicate

Click the Add button to add a new Web site to the list and make configuration settings for it. Or, select a Web site that has most of the settings you want to use for a new site, then click Duplicate to create a duplicate site. You can then make changes to the site's settings and save it as a new site.

Edit

Select a Web site and click Edit to make changes to the site. For information about changing Web site settings, see “Web Site Settings” on page 130.

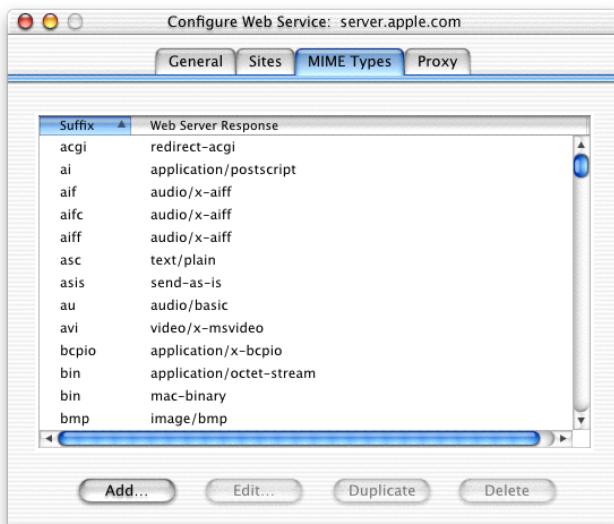
Delete

Select a Web site and click Delete if you want to remove the site from your list. You won’t remove the Web site or its contents from your server; you just delete its name and settings from the Configure Web Service list.

MIME Types Settings for Web Service

Multipurpose Internet Mail Extension (MIME) is an Internet standard for describing the contents of a file. The MIME Types pane lets you set up how your Web server responds when a browser requests certain file types. For more information about MIME types and MIME type mappings, see “Understanding Multipurpose Internet Mail Extension (MIME)” on page 141.

To access the MIME Types pane, click Web and choose Configure Web Service, then click the MIME Types tab.



Suffix

The suffix describes the type of data in a file, such as audio, text, or video.

Web Server Response

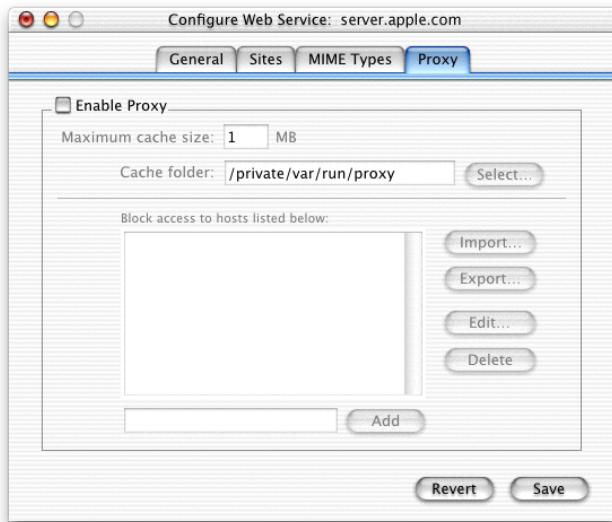
The Web server response specifies what you want the Web server to do when it receives a request for a file with the given suffix. The response can consist of an action, a response, or a combination of action and response.

Add, Edit, Duplicate, and Delete

Click these buttons to add a new MIME type, or modify existing ones.

Proxy Settings for Web Service

You can use your Web server as a proxy for your users, saving frequently accessed Web sites to a cache to improve server performance. To access the Proxy pane, click Web and choose Configure Web Service, then click the Proxy tab.



Enable Proxy

Select this checkbox to use your server as a proxy for your users. Using the server as a proxy is useful, for example, in a classroom setting where all the students are directed to the same Web sites for a project. If all the students try to connect at the same time, your server can consolidate the connection requests and cache the site, resulting in improved performance. To use proxy service, your client users need to specify your Web server as a proxy server in their Web browser preferences.

Maximum cache size

Type the maximum amount of disk space you want to use for caching requests from client computers to other Web sites. Using the cache is a way to optimize performance for a slow Internet connection. When the cache reaches the maximum size, the oldest files are deleted from the cache folder.

Cache folder

Type the path and folder name for the folder you want to use for cache storage. If file service is turned on, or if you are using Server Admin at the server, you can click the Select button to locate the folder.

Block access to hosts listed below

Click the Add button and type the domain name or IP address for any Web sites that you don't want to cache. Sites in this list will not be cached as long as the client user's Web browser lists your server as its proxy server. You may want to list objectionable Web sites here.

Import

Click this button to import a list of Web sites that you don't want to cache. The list must be a text file with the host names separated by white space (lines, spaces, or tabs).

Export

Click this button to export your list of blocked hosts to a text file.

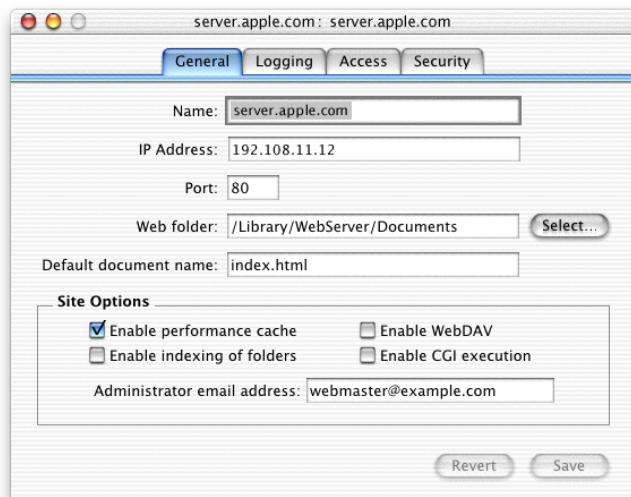
Web Site Settings

You use the site settings window to configure your Web sites. To open this window, click Web and choose Configure Web Service, then click the Sites tab. Click Add to open a new site window. Select an existing site in the list and click Edit or Duplicate to open the window for that site.

The settings window has four panes: General, Logging, Access, and Security. The settings you make here affect individual Web sites, and do not affect Web service as a whole. However, some settings are dependent on settings you make for Web service. For example, if you enable SSL for a Web site, you must also have enabled SSL for your Web service. The settings for these panes are discussed next.

General Settings for Web Sites

Use the General pane of the site settings window to set general options, such as the name and port number, for an individual Web site. To access the General pane for Web sites, click Web, choose Configure Web Service, then click the Sites tab. Click Add, or select a site and click Edit or Duplicate.



Name

Type the fully qualified domain name of the site, not just the host name. Server.apple.com is an example of a fully qualified domain name.

IP Address

Type the site's IP address. For each Web site you host, you must specify a unique IP address and port number combination, or a different host name for the server. If you set up a different IP address, the server computer must be configured to accept IP packets for multiple IP addresses. For more information about assigning multiple IP addresses, read "Setting Up Multiple IP Addresses for a Port" on page 305.

Port

Choose the port you want to use for connections to this site. By default, the server uses port 80 for all connections to Web sites on your server, but you can change the port used for an individual Web site. You can choose any number up to 8999, but make sure that the port you choose is not already in use by another service (such as FTP, Apple file sharing, and SMTP connections).

If you enable SSL for this site, you should use port 443, which is the default HTTPS port for SSL. You can find a list of TCP and UDP port numbers and the services they're used for in “Ports Used by Mac OS X Computers” on page 301.

Web folder

Type the path to the directory you want to use as the root for this site. If file service is turned on, or if you are using Server Admin at the server, you can click Select to browse for a folder.

Default document name

Type the name of the file users should see if they connect to the site using the domain name or a directory name, but no filename. When you first install the software, the default document name is “index.html.” If there is no default document, users see a directory listing (if directory listing is enabled). See “Enable detailed folder listings” on page 125 and “Enable performance cache,” below.

Note: The Default document name field can have more than one entry. Any filename containing a space must be enclosed in quotes. Each entry must be separated by a space.

Enable performance cache

Select this option if your Web site contains static HTML files and you expect high usage of the pages. Don’t enable the cache if most of your Web pages are dynamic. For more information about the performance cache, see “Disabling the Cache for Dynamic Web Pages” on page 148.

Enable indexing of folders

Select this option if you want users to see a list of the Web folder’s contents instead of the default document when they connect to this site. If indexing is not enabled and a default Web page doesn’t exist, users see a message that access is denied.

Enable WebDAV

Select this option to use WebDAV on this site. You must also enable WebDAV in the General pane of the Configure Web Service window.

Enable CGI execution

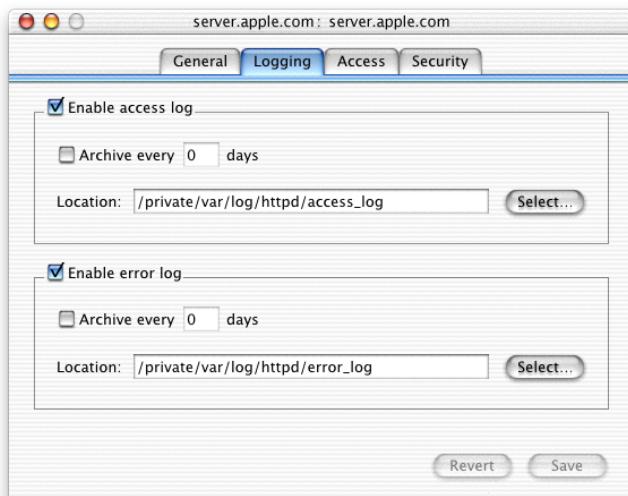
Select this option if you want to run Common Gateway Interface (CGI) programs located in your Web folder. For more information about CGI programs, see “Using a Common Gateway Interface (CGI) Script” on page 140.

Administrator email address

Type the address you want to use as the return email address in any error messages sent to a client. Apache’s default error pages include a link to the address you specify, so client users can provide feedback if they experience problems with a Web site.

Logging Settings for Web Sites

The Logging pane of the site settings window lets you set up and enable the logs for an individual Web site. To access the Logging pane, click Web, choose Configure Web Service, then click the Sites tab. Click Add, or select a site and click Edit or Duplicate. Then click the Logging tab.



Enable access log

Select this box to create a log entry each time the Web site is accessed.

Archive every _ days

Type the number of days each log file will continue to record events. At the end of the period you specify, the current log will be saved, the date added to its name, and a new log file started.

Location

Type the path and filename for the location where you want to store the log file. If file service is turned on, or if you're using Server Admin at the server, click Select and browse to find the location. The default location of log files is /var/log/httpd/

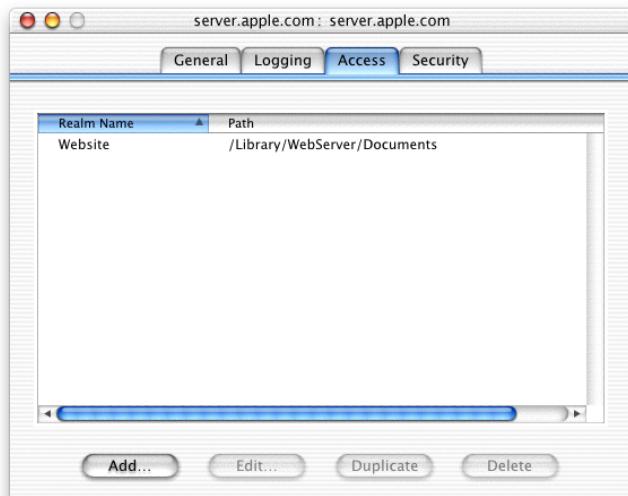
Enable error log

Click this box to log errors that occur with this Web site.

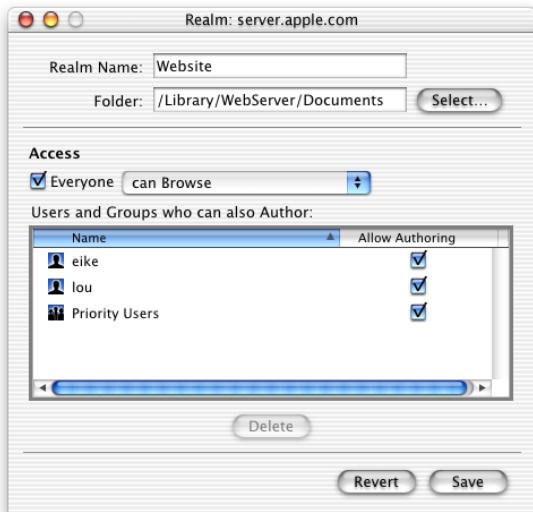
Access Settings for Web Sites

The Access pane of the site settings window lets you set up “realms,” or locations within a site. When WebDAV is enabled, users can view or make changes to these realms while the site is running. For more information about creating realms and assigning privileges, see “Understanding WebDAV Realms and Privileges” on page 149.

To find the Access pane, click Web, choose Configure Web Service, then click the Sites tab. Click Add, or select a site and click Edit or Duplicate. Then click the Access tab.



Select a realm and click Edit or Duplicate, or click Add to define a new realm using the pane shown next.



Realm Name

Type the name you want users to see when they log in. The default realm name is the name of the Web site. It's a good idea to use unique names for your realms.

Folder

Type the path to the location in a Web site to which you want to limit access. If file service is turned on, or if you are using Server Admin at the server, you can click Select and browse to find the location you want to use.

Everyone

Select this checkbox and choose the level of access you want to set for Everyone (Everyone is anyone who can access your Web site). Your two choices are “can Browse” and “can Browse and Author.” Depending on what you choose, you’ll have other choices to make:

- If you select this box and choose “can Browse,” the Users and Groups list appears below. Use this list to set authoring privileges for specific users.
- If you select this box and choose “Browse and Author,” the Users and Groups list is hidden, because there are no additional privileges to set.
- If you do not select the box, the pop-up menu is disabled, and the Users and Groups list appears below. Use this list to set browsing or authoring privileges for specific users.

Users and Groups

You can use this list to give browsing or authoring privileges to specific users. This list appears only if you set the Everyone privilege to “can Browse” or if you do not select any access privileges for Everyone. The list is empty until you drag user or group names to it from the Mac OS X Server Users & Groups List.

Allow Authoring

Select this option to assign a user or group authoring privileges for this realm.

Delete

Select a name in the Users and Groups list and click this button to deny the user or group access to this realm.

Security Settings for Web Sites

The Security pane of the site settings window lets you set up and enable secure transactions for each Web site. To access the Security pane, click Web, choose Configure Web Service, then click the Sites tab. Click Add, or select a site and click Edit or Duplicate. Then click the Security tab. For more information about setting up Secure Sockets Layer (SSL) service, see “Setting Up Secure Sockets Layer (SSL) Service” on page 142.



Enable Secure Sockets Layer (SSL)

Select this option to turn on SSL for each Web site. Make sure SSL support has been enabled for the entire Web service in the General pane of the Configure Web Service window.

Edit Certificate file

Click this button to enter the contents of your certificate file. This is the file “server.crt” that contains the Secure Server ID sent to you by the certificate authority. It’s in this directory:

/etc/httpd/ssl.crt/

Edit Key file

Click this button to enter the contents of your key file. This is the file “key.pem,” which you set up when you generated the certificate signing request (CSR).

Edit CA Certificate file

Click this button to enter the contents of the CA certificate file you received from the certificate authority. (This file is optional. For more information, see “Setting Up Secure Sockets Layer (SSL) Service” on page 142.)

Pass Phrase

Click this button to enter the SSL pass phrase you set when you generated the CSR. The pass phrase unlocks the server’s certificate key.

SSL Log file

Enter the location and name for the log file that will record SSL events. If file service is turned on, or if you are using Server Admin at the server, you can click Select to find the file you want to use.

Strategies and Tips for Web Service

There are many ways you can optimize Web service performance, prevent security holes, and customize how you administer your Web service. This section provides you with some information to help get you started, and to let you know about some things you can do beyond the basics.

Using Persistent Connections to Improve Server Performance

Normally each HTTP request and response uses a separate TCP connection. When a client computer contacts the server, the server opens a connection, retrieves the request, then closes the connection. To respond to the request, the server opens another connection, responds, then closes the connection. Repeatedly opening and closing connections isn’t very efficient and decreases performance.

Persistent connections let the server complete several transactions over one connection. Both the server and the client computer must be capable of persistent connections. (Most popular browsers support persistent connections.) For a persistent connection to work, the information that's being transmitted must be of a known size. For example, image files and static HTML pages have a known length. Common Gateway Interface (CGI) scripts and dynamically generated HTML pages don't have a known length.

You can limit the number of requests that can occur over a persistent connection. If you set the number to zero, then there is no limit to the number of requests allowed per connection. However, the default setting of 500 provides better performance.

Working With Web Modules

Modules “plug in” to the Apache Web server software and add functionality to your Web site. Apache comes with some standard modules, and you can purchase modules from software vendors or download them from the Internet. You can find information about available Apache modules at these Web sites:

- www.apache.org/docs/mod
- www.mod.apache.org

To view a list of Web modules installed on your server, click Web in Server Admin and choose Web Service Status.

To install a module, follow the instructions that came with the module software. The Web server loads modules from this directory:

/usr/libexec/httpd/

In addition, you must change the httpd.conf file to load and then add new modules.

Macintosh-Specific Modules

Web service in Mac OS X Server installs some modules specific to the Macintosh. These modules are described in this section.

mod_macbinary_apple

This module packages files in the MacBinary format, which allows Macintosh files to be downloaded directly from your Web site. A user can download a MacBinary file using a regular Web browser by adding “.bin” to the URL used to access the file.

mod_sherlock_apple

This module lets Apache perform relevance-ranked searches of the Web site using Sherlock. Once you index your site using Sherlock, you can provide a search field for users to search your Web site. You must add “.sherlock” to your site’s URL.

mod_auth_apple

This module allows a Web site to authenticate users by looking for them in directory service domains within the server's search policy. When authentication is enabled, Web site visitors are prompted for a user name and password before they can access information on the site.

The mod_redirectacgi_apple

This module works in conjunction with ACGI Enabler Application to allow users to execute ACGI programs (Mac OS CGIs). To enable an ACGI, log in as the administrator and open ACGI Enabler Application. Do not log out of the application—it must be running for ACGIs to work.

mod_hfs_apple

This module requires users to enter URLs for HFS volumes using the correct case (lowercase or uppercase). This module adds security for case-insensitive volumes. If a restriction exists for a volume, users receive a message that the URL is not found.

Open Source Modules

Mac OS X Server includes these popular open source modules: Tomcat, PHP: Hypertext Preprocessor, mod_perl, and MySQL.

Tomcat

The Tomcat module, which uses Java-like scripting, is the official reference implementation for two complementary technologies developed under the Java Community Process:

- *Java Servlet 2.2.* For the Java Servlet API specifications, see the following site:
java.sun.com/products/servlets
- *JavaServer Pages 1.1.* For these API specifications, see
java.sun.com/products/jsp

If you want to use Tomcat, you must activate it first. Follow these steps:

- 1 Open /private/etc/httpd/httpd.conf.
- 2 Uncomment the lines relating to Tomcat server configuration, or add the following lines to the end of the file:

```
LoadModule jserv_module /usr/libexec/httpd/mod_jserv.so
AddModule mod_jserv.c
Include /private/etc/httpd/tomcat.conf
```

- 3 Use Server Admin to create a virtual host site pointing to /usr/webapps/ROOT.
- 4 Start Tomcat by opening the Terminal application and entering the following:
`/usr/bin/tomcat.sh start`
- 5 Using a Web browser, enter the URL for your site to determine whether Tomcat is working as expected. (The URL looks like the following, where “example.com” is your site’s domain name.)

<http://www.example.com/>

See /etc/httpd/tomcat.conf for the Tomcat documentation and some examples.

PHP: Hypertext Preprocessor

PHP lets you handle dynamic Web content by using a server-side HTML-embedded scripting language resembling C. Web developers embed PHP code within HTML code, allowing programmers to integrate dynamic logic directly into an HTML script rather than write a program that generates HTML.

PHP provides CGI capability and supports a wide range of databases. Unlike client-side JavaScript, PHP code is executed on the server.

See www.php.net for more information about this module.

mod_perl

This module integrates the complete Perl interpreter into the Mac OS X Server, letting existing Perl CGI scripts run without modification. This integration means that the scripts run faster and consume fewer system resources. See perl.apache.org for more information about this module.

MySQL

MySQL provides a relational database management solution for your Web server. With this module, you can link data in different tables or databases and provide the information on your Web site. See www.mysql.com for more information about this module.

Using a Common Gateway Interface (CGI) Script

When users connect to your Web site, they normally receive a static html page or graphic. Common Gateway Interface (CGI) scripts, or programs, allow you to add dynamic functions to your Web site by sending information back and forth between your Web site and an application that provides a service for the site. For example, if a user fills out a form on your site, you can have a CGI send the message to an application that processes the data and sends a response back to the user. CGIs for the Mac OS are often AppleScripts, but they can also be applications.

A CGI can also perform a custom function on its own. For example, a CGI could generate a visitor count each time a user accesses the Web site, and insert the dynamically generated number onto your Web page.

To use a CGI:

Step 1: Install the CGI

You can install a CGI in one of two locations:

For only one site: Put the CGI in the Documents folder for your Web site. The CGI name must end with ".cgi." If you install the CGI here, you need to enable it for the site.

For all sites: Put the CGI in the /Library/WebServer/CGI-Executables folder. For the CGI to work on your site, you must include /cgi-bin/ in the URL for your site. You don't need to enable the CGI; if it's installed, it will run.

Step 2: Enable CGI execution for your site

In Server Admin, click Web and choose Configure Web Service, then click the Sites tab. Select a Web site in the list and click Edit. Then select Enable CGI Execution in the General pane of the site settings window.

Step 3: Restart Web service

You need to stop Web service and start it again for your changes to take effect.

Understanding Multipurpose Internet Mail Extension (MIME)

Multipurpose Internet Mail Extension (MIME) is an Internet standard for specifying what happens when a Web browser requests a file with certain characteristics. You can choose the response you want the Web server to make based on the file's suffix. Your choices will depend partly on what modules you have installed on your Web server. Each combination of a file suffix and its associated response is called a *MIME type mapping*.

MIME suffixes

A suffix describes the type of data in a file. Here are some examples:

- txt for text files
- cgi for Common Gateway Interface files
- gif for GIF (graphics) files
- au for sound files
- tiff for TIFF (graphics) files

Mac OS X Server installs a default list of MIME type suffixes. If a suffix you need is not listed, you can use Server Admin to add it to the list.

Web server responses

When a file is requested, the Web server handles the file using the response specified for the file's suffix. Responses can be either an action or a MIME type. Possible responses include

- return file as MIME type (you enter the mapping you want to return)
- send-as-is (send the file exactly as it exists)
- cgi-script (run a CGI script you designate)
- imap-file (generate an IMAP mail message)
- mac-binary (download a compressed file in MacBinary format)

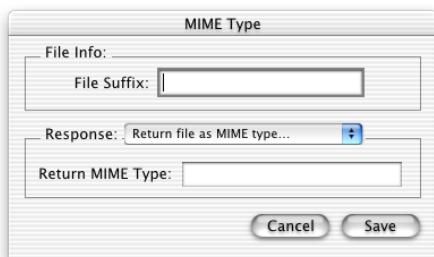
MIME type mappings are divided into two subfields separated by a forward slash, such as “text/plain.” Mac OS X Server includes a list of default MIME type mappings. You can edit these or add others.

When you specify a MIME type as a response, the server identifies the type of data requested and sends the response you specify. For example, if the browser requests a file with the suffix “jpg,” and its associated MIME type mapping is “image/jpeg,” the server knows it needs to send an image file and that its format is JPEG. The server doesn’t have to do anything except serve the data requested.

Actions are handled differently. If you’ve mapped an action to a suffix, your server runs a program or script, and the result is served to the requesting browser. For example, if a browser requests a file with the suffix “cgi,” and its associated response is the action “cgi-script,” your server will run the script and send the resulting data back to the requesting browser.

MIME Type editor

You can create MIME types and map them to server responses using Server Admin. To access the MIME Type editor, click Add in the MIME Types pane, or select an existing MIME type and click Edit. The editor is shown here.



Setting Up Secure Sockets Layer (SSL) Service

If you want to provide secure transactions on your server, such as allowing users to purchase items from a Web site, you should set up Secure Sockets Layer (SSL) protection. SSL lets you send encrypted, authenticated information across the Internet. So if you want to allow credit card transactions through a Web site, for example, you can protect the information that’s passed to and from that site.

When you generate a certificate signing request (CSR), the certificate authority sends you a certificate that you install on your server. They may also send you a CA certificate (ca.crt); installing this file is optional. Normally, CA certificates reside in client applications such as Internet Explorer and allow those applications to verify that the server certificate originated from the right authority. However, CA certificates expire or evolve, so some client applications may not be up-to-date.

To set up SSL, follow these steps:

Step 1: Generate a certificate signing request (CSR) for your server

The CSR is a file that provides information needed to set up your server certificate.

To generate a CSR for your server:

- 1 Log in to your server using the root password and open the Terminal application.
- 2 At the prompt, type these commands and press Return at the end of each one.

```
cd  
openssl md5 * > rand.dat  
openssl genrsa -rand rand.dat -des 1024 > key.pem
```

- 3 At the next prompt, type a pass phrase, then press Return.

The pass phrase you create unlocks the server's certificate key. You will use this pass phrase when you enable SSL on your Web server.

- 4 If it doesn't already exist on your server, create a folder with the following name:

```
/etc/httpd/ssl.key/
```

Make a copy of the key.pem file (created in step 2) and rename it "server.key." Then copy server.key to the folder.

- 5 At the prompt, type the following command and press Return.

```
openssl req -new -key key.pem -out csr.pem
```

- 6 When prompted, enter the following information:

- *Country*: This is the country in which your organization is located.
- *State*: Type the full name of your state.
- *Locality*: This is the city in which your organization is located.
- *Organizational name*: This must be the organization to which your domain name is registered.
- *Organizational unit*: This is usually something similar to a department name.
- *Common name of your Web server*: This is the DNS name, such as server.apple.com
- *Email address*: The email address to which you want the certificate sent.

The file "csr.pem" is generated from the information you provided. At the prompt, type the following, then press Return.

```
cat csr.pem
```

The cat command lists the contents of the file you created in step 5 (csr.pem). You should see the phrase "Begin Certificate Request" followed by a cryptic message. The message ends with the phrase "End Certificate Request." This is your certificate signing request (CSR).

Step 2: Obtain a Web site certificate

You must purchase a certificate for each Web site from an issuing authority.

Keep these important points in mind when purchasing your certificate:

- You must provide an InterNIC-registered domain name that's registered to your organization.
- If you are prompted to choose a software vendor, choose Apache Freeware with SSLeay.
- You already generated a CSR, so when prompted, open your CSR file using a text editor, then copy and paste the contents of the CSR file into the appropriate text field on the issuing authority's Web site.

After you've completed the process, you'll receive an email message that contains a Secure Server ID. This is your server certificate. When you receive the certificate, save it to your Web server's hard disk as a file named "server.crt."

Step 3: Install the certificate on your server

- 1** Log in to your server as root.
- 2** If it doesn't already exist on your server, create a folder with this name:
/etc/httpd/ssl.crt/
- 3** Copy server.crt (the file that contains your Secure Server ID) to the folder.

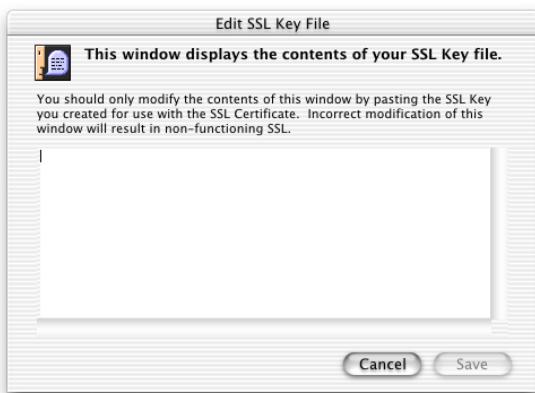
Step 4: Enable SSL for the site

- 1** In Server Admin, click Web and choose Configure Web Service.
- 2** Make sure Enable SSL support is selected for the entire site.
- 3** Click Sites, then select the site where you plan to use the certificate, and click Edit.
- 4** Select Enable Secure Socket Layer (SSL).

- 5** Click Edit Certificate File and paste the text from your certificate file (the certificate you obtained from the issuing authority) in the text field, then click Save.



- 6** Click Edit Key File and paste the text from your key file (the file key.pem, which you set up earlier) in the text field, then click Save.



- 7** Click Edit CA Certificate File and paste the text from the ca.crt file in the text field. (This is an optional file that you may have received from the certificate authority.) Click Save.



- 8** Press tab to move to the Pass Phrase field and type the pass phrase from your CSR in the text field, then click OK.
- 9** Set the location of the log file that will record SSL transactions and click Save.
- 10** Stop and then start Web service.

Monitoring Service Activity and Performance

Web service provides three useful tools to help you monitor your server activity and keep it running efficiently: access and error logs, and the status window.

Access and error logs

You can view Web service access and error logs remotely using Server Admin. Click Log Viewer and choose Web Service, then choose access.log or error.log from the pop-up menu. Depending on the size and purpose of your Web site, it is likely that your logs will contain a large number of entries. Web service in Mac OS X Server uses the standard Apache log format, so you can use any third-party log analysis tool to interpret the log data. You can designate a location for your log files using the Logging pane in the site settings window. The default location is /var/log/httpd/.

Status window

You can also monitor server activity using the Web Service Status window in Server Admin. To open this window, click Web and choose Show Web Service Status. The Web Service Status window shows the current state of the server and the performance cache. If Web service isn't running, the window displays "Status: not running," and the date and time the server stopped.

When Web service is running, the window looks similar to the one below. Messages about server status show in the Start/Stop Status Messages field—you can check the Apache Web site for explanations if you’re not sure what they mean.

Current requests and current throughput include both Apache and performance cache data. Performance cache requests and throughput include performance cache data only.



Advanced Apache Configuration

If you are an expert Apache Web administrator, you may want to configure Web service by modifying the Apache configuration file, httpd.conf. If you plan to make a lot of modifications, you should configure your Web service using only the Apache configuration file, rather than Server Admin.

Configuration settings (directives) you make using Server Admin are written to the Server Admin configuration file, httpd_macosxserver.conf. To help you avoid making duplicate, and possibly conflicting, directives, settings that can be made in Server Admin appear in the Apache configuration file with a pound sign (#) in front of them. Apache ignores any directives preceded by the pound sign.

For example, the directive for persistent connections (KeepAlive) appears in the Apache configuration file (httpd.conf) as this:

```
#KeepAlive Off
```

However, if you enable persistent connections in Server Admin, the httpd_macosxserver.conf file contains this:

KeepAlive On

Since the “disable” directive is preceded by a pound sign in the Apache configuration file, there is no conflict. Apache will read only the directive contained in the Server Admin configuration file.

Important All settings used by Server Admin appear in the httpd.conf file with a pound sign (#) in front of them. Do not modify these, or you could have unexpected results with your Web service.

Warning You should not, under any circumstances, modify the file
httpd_macosxserver.conf.

For more information on Apache and how to use it, refer to the Apache Web site at www.apache.org

Disabling the Cache for Dynamic Web Pages

If you have dynamic Web pages on your site (such as pages generated by CGI scripts or databases that update frequently), you need to make sure those pages are not kept in the cache. Otherwise you may provide old or incorrect information on your site.

Your Web server is set up so that any HTML file on your server automatically has an added tag that indicates when the file should expire in the cache. By default, HTML pages expire from the cache after 1 second, and GIF files expire after one hour.

If your site is serving old or incorrect information, you can do one of the following:

- Verify that the performance cache is not enabled in the Configure Web Service window of Server Admin.
- Modify your CGI scripts (or any program you use to generate dynamic HTML pages) so the scripts add a “Cache-Control: no-cache” tag in the source of each dynamic HTML page.
- Check the httpd.conf file to see if GIF files are being cached.

If GIF files are being cached and you want to prevent this, you can modify the httpd.conf file. Here’s how to do it:

- 1 Open the httpd.conf file using a text editor.
- 2 Find this line:

```
ExpiresByType image/gif A3600
```

This command tells the Web server to assign GIF files a one-hour (3600 seconds) caching duration.

- 3** Insert a pound sign (#) at the start of the line so it looks like this:

```
#ExpiresByType image/gif A3600
```

Inserting the pound sign causes Server Admin to ignore the directive to cache GIF files, so GIF files are no longer cached.

- 4** Restart Web service.

Understanding WebDAV Realms and Privileges

If you use WebDAV to provide live authoring on your Web site, you should create realms and set access privileges for users. Each site you host can be divided into a number of realms, each with its own set of users and groups that have either browsing or authoring privileges. If your Web site is on an intranet, you may not want to create realms.

Defining Realms

When you define a realm, which is typically a folder (or directory), the access privileges you set for the realm apply to all the contents of that directory. If a new realm is defined for one of the folders within the existing realm, only the new realm privileges apply to that folder and its contents. For information about creating realms and setting access privileges, see “Access Settings for Web Sites” on page 134.

Setting WebDAV Privileges

The Apache process running on the server needs to have access to the Web site’s files and folders. To do this, Mac OS X Server installs a group named “www” made up of the Apache processes in the server’s Users & Groups List. You need to give the www group Read access to files within Web sites so that it can transfer the files to browsers when users connect to the sites. If you’re using WebDAV, the www group also needs Write access to the files and folders in the Web sites.

Solving Problems With Web Service

If users can’t connect to a Web site on your server:

- Make sure that Web service is turned on and the site is enabled.
- Check the Start/Stop Status Messages field in the Web Service Status window for messages. If you are not sure what the messages mean, you’ll find explanations on the Apache Web site (www.apache.org).
- Make sure users are entering the correct URL to connect to the Web server.
- Make sure that the correct folder is selected as the default Web folder. Make sure that the correct HTML file is selected as the default document page.
- If your Web site is restricted to specific users, make sure those users have access privileges to your Web site.

- Verify that users' computers are configured correctly for TCP/IP. If there doesn't appear to be a problem with the TCP/IP settings, use a "pinging" utility that allows you to check network connections.
- Verify that the problem is not a DNS problem. Try to connect with the IP address of the server instead of its DNS name.
- Make sure your DNS server's entry for the Web site's IP address and domain name are correct.

If a Web module is not working as expected:

- Check the error log in the Log Viewer for information about why the module might not be working correctly.
- If the module came with your Web server, check the Apache documentation for that module and make sure the module is intended to work the way you expected.
- If you installed the module, check the documentation that came with the Web module to make sure it's installed correctly and is compatible with your server software.

For more information on supported Apache modules for Mac OS X Server, see this Web site:
www.apache.org/docs/mod/

If a CGI will not run:

- Check the CGI's code to make sure it's marked as executable. If it's not, it won't run on your server even if you enable CGI execution in Server Admin.
- Check the CGI's code to see if appropriate access has been granted. Mac OS X Server installs a group named "www" made up of the Apache processes in the server's Users & Groups List. A CGI must give appropriate access (Read Only, or Read & Write) to the www group.

Web Service Specifications

Maximum number of concurrent connections	No technical limit; depends on your hardware's capabilities and how you set up your server software
Supported standards	Fully compatible with HTTP 1.1 and earlier
Maximum server name length for network services	Determined by Network Service Locator (NSL)
Idle connection timeout	60 seconds (you can reset)
CGI timeout	60 seconds
Web service port number	80 (you can reset)

Where to Find More Information About Web Service

For information about configuration files and other aspects of Apache Web service, see these resources:

- *Apache: The Definitive Guide*, 2nd Edition, by Ben Laurie and Peter Laurie (O'Reilly and Associates, 1999)
- *Writing Apache Modules with Perl and C*, by Lincoln Stein and Doug MacEachern (O'Reilly and Associates, 1999)
- *Web Performance Tuning*, by Patrick Killelea (O'Reilly and Associates, 1998)
- *Web Security & Commerce*, by Simson Garfinkel and Gene Spafford (O'Reilly and Associates, 1997)
- For more information about Apache, see the Apache Web site: www.apache.org
- For an inclusive list of methods used by WebDAV clients, see RFC 2518. RFC documents provide an overview of a protocol or service that can be helpful for novice administrators, as well as more detailed technical information for experts. You can search for RFC documents by number at this Web site: www.faqs.org/rfcs

Mail Service

What Is Mail Service?

Mail Service in Mac OS X Server allows you to provide email service for users over your network or across the Internet. If you want your users to be able to send and receive mail over the Internet, you can set up mail service using all of the standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP).

A standard mail setup uses SMTP to send email, and POP and IMAP to receive messages at the local server. The three protocols are described next.

Post Office Protocol

Post Office Protocol (POP) is used to receive, but not send, mail. POP delivers mail to a shared server, and users' computers connect to the server periodically to download all of their waiting mail. Once the user has downloaded mail, the mail is stored only on the user's computer, and the user can disconnect from the mail server and read, organize, and reply to mail, or compose new mail. POP is like a post office, storing mail and delivering it to a specific address.

One advantage of POP is that your mail 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 the IMAP protocol. However, because the mail is removed from the server, if any client computers sustain hard disk damage and lose their mail files, there is no way you can recover these files without using data backups.

POP is not the best choice for client users who access mail from different locations, such as home, the office, or on the road with a mobile device. When a user reads mail, it is downloaded and completely removed from the server. If the user logs in later from a different computer, he or she won't be able to see previously read mail.

Internet Message Access Protocol

Internet Message Access Protocol (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 industry-standard Internet mail programs, or any IMAP-compliant email client.

With IMAP, client users' mail is stored in a remote mailbox on the server; mail appears to users just as if it were on the local computer. IMAP delivers mail to the server, as with POP, but the mail is not removed from the server until the user deletes it.

IMAP is more like the typical client-server model, where the user's computer can ask the server for headers, or the bodies of specified messages, or search for messages that meet certain criteria. These messages are downloaded as the user opens them.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol that is used to send and transfer mail. Since its ability to queue incoming messages is limited, it is usually used only to send mail, while POP or IMAP is used to receive mail.

Before You Set Up Mail Service

How you manage mail service depends on how you organize your mail server. Read this section for information about using mail service on your network. You can install and run Mac OS X mail service on a single server or on multiple servers.

Mail Service for a Single Server

When mail service is provided by a single server, all users send messages to the same mail server. Messages are stored there until a user's mail application requests that messages be downloaded to the user's computer.

Mail Service for Multiple Domains

You can also use Mac OS X Server to set up mail service for more than one domain. For example, if you are providing mail service to several companies in your building, each with its own domain name, you can set up mail service for each domain.

Or, if your organization has more users than your mail server's concurrent user connection limit (which is influenced by connection type—POP or IMAP—and server usage), or more messages than the message storage limit, you may want to distribute your mail service across multiple servers.

Sharing mail service across servers improves performance (including the number of connections and messages the mail system can handle), but you need to more carefully manage the Users & Groups database, DNS entries, and mail servers.

When mail service is shared among multiple servers, the servers participate in a store-and-forward operation. Each mail server stores incoming messages for the users who connect to it, and forwards incoming messages addressed to users who connect to other servers.

MX Records for Internet-Based Mail Service

When you set up mail service, incoming mail is delivered to a computer (or mail host), where it waits until a user connects to the host and retrieves the mail. You should also set up an alternate computer to receive mail if the mail host is not available. Outgoing mail is sent from a user's computer to an outgoing mail host, which then sends the mail to another mail host on the Internet. The mail is passed along until it reaches the mail host that holds mail for the user to which it is addressed.

To provide mail service, you need a computer that can provide Domain Name System (DNS) service for your network. The mail server relies on DNS to obtain IP addresses of other mail servers. If you're providing mail service over the Internet, you need to set up DNS service with appropriate Mail Exchange (MX) records for each domain for which you're providing mail service. MX records are entries in a DNS table that specify how mail is handled for a domain. When another mail server on the Internet has mail to deliver to your domain, it requests the MX record for your domain, and the record directs the mail to the mail server you specified in the MX record.

For more information about creating MX records, see “Using DNS With Mail Service” on page 282.

Setting Up Mail Service for the First Time

Step 1: Set up MX records

If you want users to be able to send and receive mail over the Internet, you need to make sure DNS service is set up with the appropriate MX records for your server. If you have an Internet service provider (ISP) who provides DNS service to your network, contact the ISP and have them set up MX records for you. For more information about DNS, see “Domain Name System (DNS) Service” on page 280.

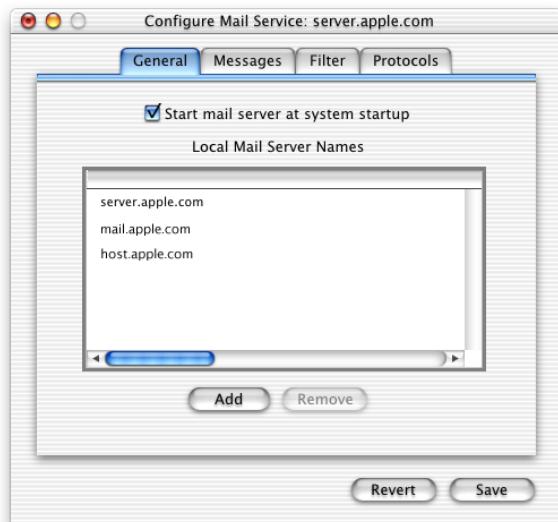
Step 2: Start mail service

Make sure the server computer shows the correct day, time, time zone, and daylight-saving settings in Date & Time Preferences. Mail service uses this information to time stamp each message. An incorrect time stamp may cause other mail servers to handle a message incorrectly.

Once you've verified this information, click Mail and choose Start Mail Service. If you asked the Setup Assistant to turn mail service on, stop it and then start it again for your changes to take effect.

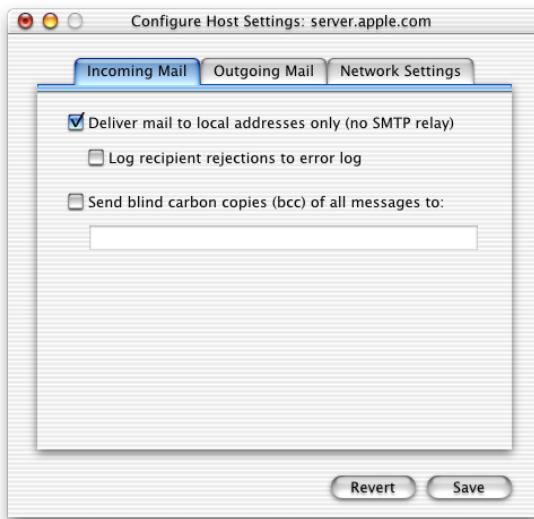
Step 3: Configure mail service

You need to select certain settings for your mail service, such as how mail is handled, which protocols you want to enable, and how often mail is deleted from the server. In Server Admin, click Mail and choose Configure Mail Service. The Mail Server Settings window (shown below) has four panes: General, Messages, Filter, and Protocols. Click each of these and choose the settings you need. For more information about these settings, see “Mail Service Settings” on page 158.



Step 4: Select default host settings

A host is any domain from which your users have received mail, or to which they have sent mail. You need to select default settings for how you want your mail service to interact with other hosts. To do this, click Mail in Server Admin and choose Configure Host Settings. The Default Host Settings window (shown below) has three panes: Incoming Mail, Outgoing Mail, and Network Settings. Click each of these and choose the settings you want. For more information about these settings, see “Host Settings” on page 166.



Step 5: Enable mail for users and create a postmaster account

The mail server uses information in Users & Groups to determine how to handle mail for your users. You can set up mail for a single user when you create a user record, or you can enable mail service for an existing user at any time. For instructions on defining mail attributes for individual users, see “Mail Service Settings” on page 65 of the Users & Groups chapter.

You also need to create a user account named “postmaster.” The mail server looks for this user when it performs certain operations. You can enable mail for the postmaster, and forward mail directed to the postmaster to another mail account.

Note that “postmaster” contains 10 characters, whereas short names are limited to 8 characters. When setting up the Mail Server, you can use a user’s long name, and are not limited to the eight-character short name. Create a user with the long name “postmaster”, and give it a short name such as “postmstr”.

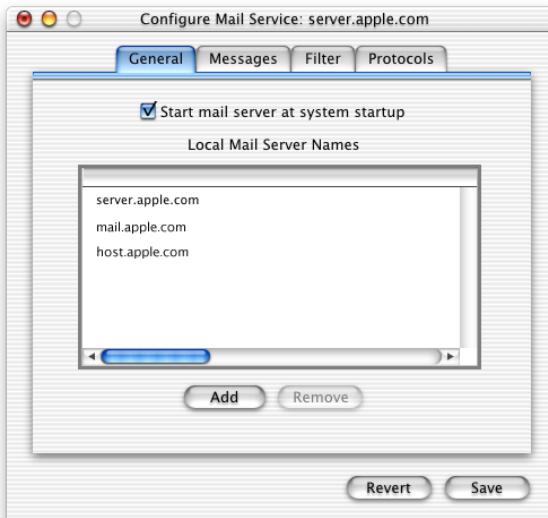
Mail Service Settings

Mail service settings let you configure how your server handles mail. You can designate local mail server names, set how the server handles message storage and error logging, and specify which mail protocols and junk mail filter techniques to use.

To access the mail settings, click Mail and choose Configure Mail Service. Click a tab to see the settings in that pane. The settings available in each pane are described in the following sections.

General Settings

You use the general settings to enable automatic startup and register local mail server names.



Start mail server at system startup

Select this option if you want mail service to start whenever the server starts up. Choosing this option ensures that your users will still have mail service after a power outage or other unexpected event.

Local Mail Server Names

This list contains all the domain names your mail server is responsible for. You should add any names that are likely to appear after @ in the addresses of mail directed to your server. For example, the list might contain variations of the spelling of your domain name or company name. Your mail settings apply to any domain names in this list. If you've set up MX records, you don't need to add anything to this list. Your mail server will add names as it discovers them in the course of its daily operation.

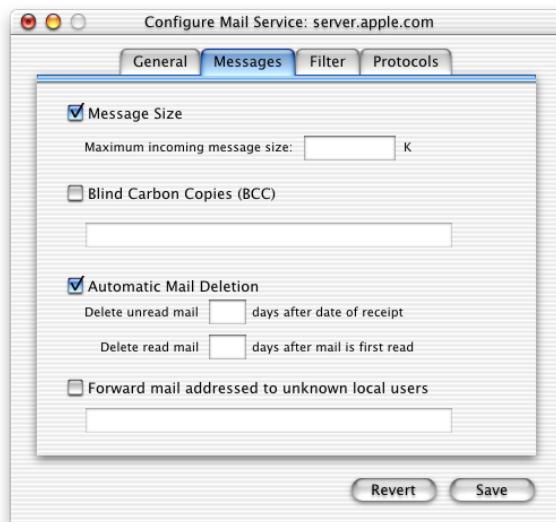
If a domain name in this list does not have an MX record, it is only recognized by this mail server. External mail sent to this domain name will be returned. You should only place domain names without MX records in this list as a time saver for local (internal) mail.

Add and Remove

Click Add and type the domain name that you want the server to be responsible for in the text field. If you want to remove a name from the list, select it and click Remove.

Messages Settings

To access the Messages pane, click Mail and choose Configure Mail Service, then click the Messages tab. You use this pane to specify a size limit for messages, set up blind carbon copies and forwarding, and schedule mail deletion.



Message Size

Select this option if you want to set an upper limit on the size of incoming messages. Then enter a number of kilobytes in the “Maximum incoming message size” box.

Blind Carbon Copies (BCC)

Select this option if you want to send blind carbon copies of all messages received by the server to a specific user or group, then type the user or group name in the text field (or you can drag a user or group name from the Mac OS X Server Users & Groups List). You might want to choose this option if you need to monitor messages sent to a group. Be aware that, depending on the size of your organization, this could generate a lot of mail.

Automatic Mail Deletion

Select this option if you want to have mail deleted from the server automatically after a specified period of time. Then enter the number of days in the fields for unread and read mail. (Don't enter a number of days if you don't want to enable one of the settings.) You may want to set these options if disk space is an issue. Automatic mail deletion permanently removes mail from the server, including messages in IMAP folders.

Forward mail addressed to unknown local users

Select this option if you want mail that arrives for an unknown local user to be forwarded to another person or a group in your organization. Type the user or group name in the text field. This person or group will receive all the misdirected mail.

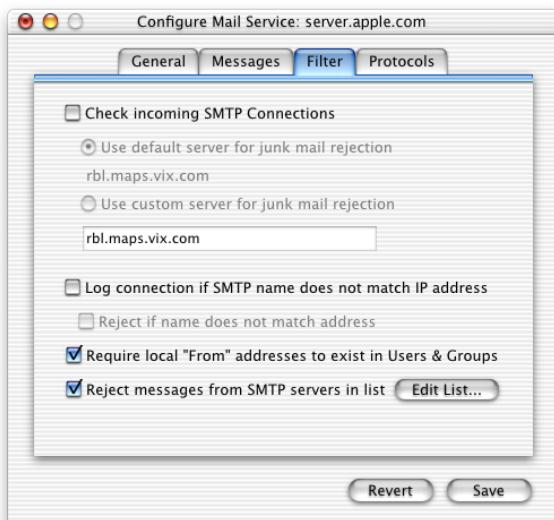
You might use this option to ensure delivery of mail with errors in the address. If someone sends mail to your server with a misspelled name, you can manually deliver the mail to the user's mailbox instead of bouncing it back to the sender. You can also direct mail sent to a department with no user account, such as "support@example.com," to the person responsible for that department's communications.

Filter Settings

You can configure filter settings for mail service to decrease the volume of unsolicited mail. If you enable any of these options, your server will check DNS entries to see if the IP address and name of a message's sender match, or will check an Open Relay Behaviour-modification System (ORBS) server to see if the message came from a known "junk mail" sender.

You should be aware that because these operations involve contacting DNS, they could slow down the performance of your mail server.

To access the Filter pane, click Mail and choose Configure Mail Service, then click the Filter tab.



Check incoming SMTP Connections

Select this option if you want to check incoming connection attempts before accepting or rejecting them. If you select this option, you also need to specify which mail server you want to use to reject mail. You can choose the default ORBS server, or choose another ORBS server by selecting “Use custom server for junk mail rejection” and typing the server name in the text field.

Log connection if SMTP name does not match IP address

Select this option if you want to create a log entry whenever an incoming message has an SMTP name that does not match the IP address. The mail is still accepted, but an entry is written to the log so you can decide later what to do about it.

Reject if name does not match address

Select this option if you want to reject mismatched mail as well as log it.

Require local “From” addresses to exist in Users & Groups

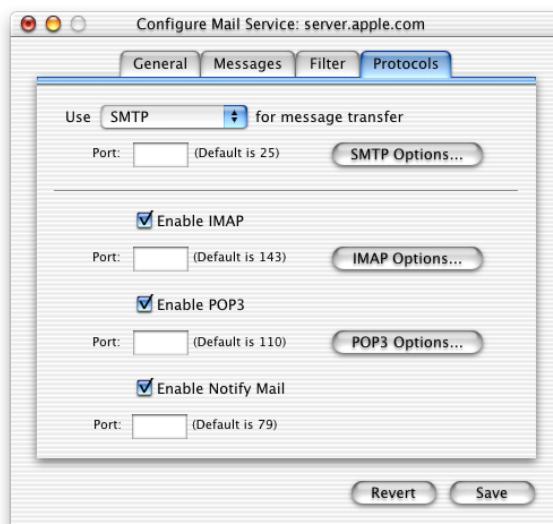
Select this option to refuse incoming mail from addresses that are not included in the local Users & Groups List. For example, if the user “Someone” sends mail from someone@example.com, and Someone is not in your Users & Groups List, the mail server rejects the message. Using this setting helps prevent your server from being used as a relay point for junk mail. A relay point is a server that unknowingly receives and immediately forwards junk mail messages to another server.

Reject messages from SMTP servers

Select this option if you want to list SMTP servers from which you don't want to receive mail. Then click Edit Servers and add domain names to the SMTP Server Rejection List.

Protocols Settings

You can select and configure the mail protocols you want your server to use in the Protocols pane. To access the Protocols pane, click Mail and choose Configure Mail Service, then click the Protocols tab.



Use _ for message transfer

Choose how you want to handle outgoing messages. You can choose SMTP, Sendmail, or None. If you choose SMTP, the SMTP Options button is active.

If you choose Sendmail, all incoming and outgoing SMTP mail is handled by Sendmail, rather than the Mac OS X mail server. Any mail sent to local email users is processed by the Sendmail application, and transferred to the Mac OS X mail server for delivery. POP and IMAP continue to function as usual, but SMTP mail is now subject to the rules and settings of the Sendmail application.

Choose None if you need to prevent new outgoing mail from being sent. You might want to do this to isolate a problem, or to prevent conflicts with other mail service software running on the same computer.

Incoming Mail Options

Select the Enable button to use IMAP, POP3, and NotifyMail. Then choose the port that you want to use for each. The default port for each is shown next to the Port field. You can choose your own port, but do so carefully. You may prevent mail from being delivered to other hosts because they aren't expecting mail to come from ports other than the expected ports. Also, don't use a port that is used by another service. For a list of common port usage, see "Ports Used by Mac OS X Computers" on page 301.

Each protocol has its own Options button to let you select further settings. These options panes are discussed in the following sections.

Enable NotifyMail

Select this option if you want your server to notify users when they have mail waiting for them. Then choose the port to use for this feature.

SMTP Options Settings



Incoming response name

Enter the domain name you want to send back to the contacting server when a network operation using SMTP takes place. The default for this setting is the primary mail server's name. Changing this name may help limit unsolicited mail by hiding the mail server's true identity.

Outgoing response name

Enter the domain name that you want outside hosts to see. This name will be appended to outgoing mail messages. There are advantages and disadvantages to changing this name. If you have a Network Address Translation (NAT) firewall on your network, you may be required to change it. But if you do, some mail servers may reject your mail because they don't recognize the address from which it came.

Allow SMTP relay when host is a backup for destination

Select this option if you want to act as a backup for another mail server, but don't want to apply your junk mail filter settings to the other host's mail.

Send undeliverable non-delivery reports to postmaster

Select this option if you want the postmaster to be notified when mail is not deliverable, and the sender cannot be notified. Normally, a report is sent back to the sender to let them know the mail was undeliverable. If for some reason the report can't be delivered, selecting this option will send the report to the postmaster account. Make sure you've set up a user account named "postmaster" in Users & Groups.

Allow non-delivery reports for bulk mail

Select this option if you want senders of bulk mail to receive nondelivery reports. Normally, mail marked as "bulk" does not generate nondelivery reports.

IMAP Options Settings



Incoming response name

Enter the domain name you want to send back to the connecting IMAP client when a network operation using IMAP takes place.

Allow IMAP Administrator Access

Select this option if you want to allow a mail service administrator to view and modify the contents of the mail database.

Port

Type the port number that you want the administrator to use to view IMAP messages. If you choose a port other than the default, make sure you are not using a port already in use by another service or protocol. You should also set up IP filter service for this port for added security. For a list of common port usage, see “Ports Used by Mac OS X Computers” on page 301.

Use case-sensitive IMAP folder names

Select this option if you want to allow users to create IMAP folders with the same name, but different cases. For example, a user could have two different folders named “Urgent” and “urgent.”

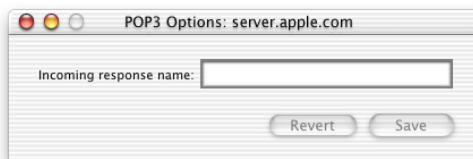
Allow _ Connections per user on a single IP address

Type the number of IMAP connections you want to allow each user to have on a single IP address. The default setting is 32. The accepted range is 1 through 999.

Terminate connections after _ minutes

Type the number of minutes you want to allow connections to remain idle before they are terminated. The default is 30 minutes. The accepted range is 1 through 999. Terminating idle connections can improve mail service performance.

POP3 Options Settings



Incoming response name

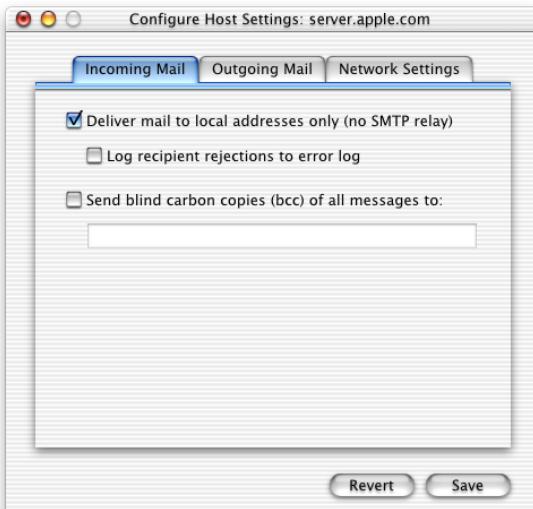
Enter the domain name you want to send back to the connecting POP client when a network operation using POP takes place.

Host Settings

You can create default settings for mail hosts in the Default Host Settings window. To access the Default Host Settings window, click Mail and choose Configure Host Settings. The three panes—Incoming Mail, Outgoing Mail, and Network Settings—are described in the following sections.

Incoming Mail Settings

You use this pane to configure how hosts handle incoming mail. To access the Incoming Mail pane, click Mail and choose Configure Host Settings, then click the Incoming Mail tab.



Deliver mail to local addresses only (no SMTP relay)

Select this option if you want the mail server to restrict delivery of mail to valid addresses on this mail server only. You should only choose this option if this host is the end point, or final delivery point, of mail.

Important If this mail server is designated as a backup server for another host, or an SMTP relay server for other servers, choosing this option could prevent mail from being sent to the other host.

Log recipient rejections to error log

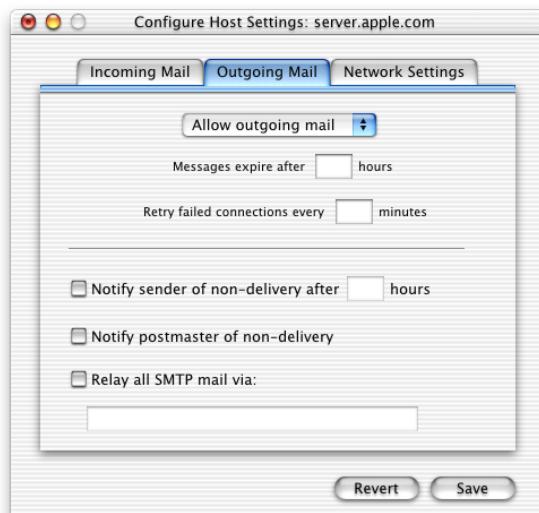
Select this option if you want to create an entry in the error log whenever mail is rejected.

Send blind carbon copies (bcc) of all messages to

Select this option if you want blind carbon copies of all incoming messages to be sent to a single address or group that you specify. Type a user or group name in the box.

Outgoing Mail Settings

You use this pane to configure how hosts handle outgoing mail. To access the Outgoing Mail pane, click Mail and choose Configure Host Settings, then click the Outgoing Mail tab.



Allow outgoing mail

Choose this option from the pop-up menu if you want to allow mail to be sent outside the host's domain.

Limit to local users

Choose this option from the pop-up menu if you want to restrict outgoing mail to the host's domain. If you choose this option, the rest of the options in this pane will be unavailable. Use this option for users on a local area network (LAN), but not for another SMTP server.

Messages expire after _ hours

Enter the number of hours you want your server to wait before it stops trying to deliver a message. The default is 72 hours. If mail can't be delivered within the time you specify, a nondelivery report is sent to the user and the message is deleted.

Retry failed connections every _ minutes

Enter the number of minutes that you want your server to wait between connection attempts to other SMTP servers. The smallest number allowed is one minute; the default is 20 minutes.

Notify sender of non-delivery after _ hours

Select this option if you want to notify the sender that a message has not yet been delivered. Then enter the number of hours you want to wait before notifying the sender. Your server will continue trying to deliver the message until it reaches the time limit you set in “Messages expire after _ hours.” The default is four hours.

Notify postmaster of non-delivery

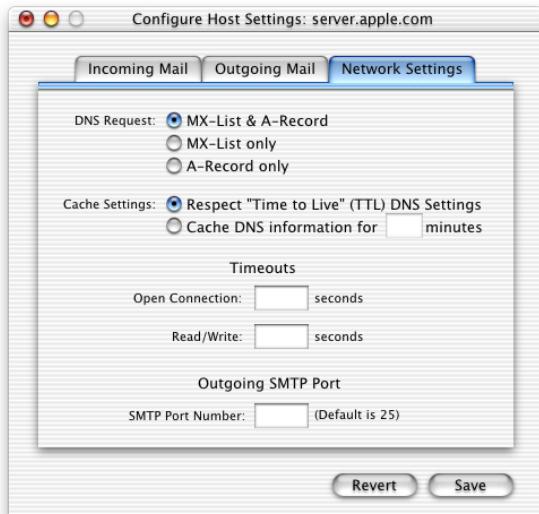
Select this option if you want the postmaster to be notified when mail can't be delivered. Normally, a report is sent back to the sender to let them know the mail was undeliverable. If for some reason the report can't be delivered, this option sends the report to the postmaster account. Make sure you've set up a user account named “postmaster” in Users & Groups.

Relay all SMTP mail via

Select this option if you want all outgoing mail to be routed through another server. Enter the server's DNS name in the text field. Your server will batch outgoing mail and send it to the other server, which acts as a proxy for delivering the mail. You may find this setting useful if you have a slow connection, or are billed by the number of connections you initiate. You may need to use this setting to get around certain firewall restrictions.

Network Settings

You use this pane to choose the outgoing SMTP port and set options for DNS, caching, and timeouts. To access the Network Settings pane, click Mail and choose Configure Host Settings, then click the Network Settings tab.



DNS Request

Choose the type of DNS records you want to request for your service. You can choose A-record, MX-List, or both. An A-record matches a host name to an IP address. MX records are entries in a DNS table that specify which computers to route mail to in a domain. You can read more about MX records on page 155.

Cache Settings

The server stores verified domain names in a cache and does not verify the information again unless you direct it to. This feature improves performance, since your mail server doesn't have to contact the DNS server for every message. You have a choice of what to set for the cache:

Respect "Time to Live" (TTL) DNS Settings: Select this setting if you want to use the default DNS settings. Normally, mail is resent continually until a connection is made. TTL sets a limit on how often the server contacts DNS for information before it gives up and a nondelivery report is generated.

Cache DNS information for _ minutes: Select this option if you want to periodically update the DNS information in the cache. Then enter the number of minutes that you want to hold information in the cache. This overrides the default TTL DNS setting.

Timeouts

Whenever a connection attempt takes longer to complete than the amount of time you specify, the connection attempt is stopped and you're notified that the connection "timed out." You may want to increase these time limits if you have a slow or intermittent connection and are experiencing frequent timeouts.

Open Connection: Type the number of seconds you want to allow for connections to be completed.

Read/Write: Type the number of seconds you want to allow for messages to be read and written before they "time out" and the connection is dropped.

Outgoing SMTP Port

Enter the port number you want to use for outgoing SMTP packets. If you choose a port other than the default, make sure you are not using a port already in use by another service or protocol.

Where to Find More Information About Mail Service

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

- A good all-around introduction to mail service can be found in *Internet Messaging*, by David Strom and Marshall T. Rose (Prentice Hall, 1998).
- For more information on 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 may be *Removing the Spam: Email Processing and Filtering*, by Geoff Mulligan (Addison-Wesley Networking Basics Series, 1999).
- To learn about email standards, see *Essential E-Mail Standards: RFCs and Protocols Made Practical*, by Pete Loshin (John Wiley & Sons, 1999).

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

Request for Comments (RFC) documents provide an overview of a protocol or service and details about how the protocol should behave. If you are a novice server administrator, you probably find some of the background information in an RFC helpful. If you are an experienced server administrator, you can find all the nitty-gritty technical details about a protocol in its RFC document. You can search for RFC documents by number at this Web site: 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

For simple explanations about mail service, see this Web site:

- www.whatis.com

Search for any technical term to find a simple explanation of the term. Also, this Web site offers a set of links to more detailed information about how a particular technology works.

QuickTime Streaming Server

What Is QuickTime Streaming Server?

QuickTime Streaming Server (QTSS) is a technology that lets you deliver media over the Internet in real time. With streaming, your users can tune in to broadcasts of live or prerecorded media, or they can view prerecorded media on demand. Users see streamed media as soon as it reaches the computer; they don't have to wait to download files.

Here are some of the key features of QuickTime Streaming Server:

- Skip Protection, available when streaming clients are using QuickTime 5, protects streams from disruptions and congestion on the Internet, resulting in higher quality.
- Two schemes of authentication, Digest and Basic, provide flexibility in controlling access to protected media.
- The playlists feature lets you easily stream a set of media files as if it were a live broadcast. This can be ideal for creating and managing a virtual radio station.
- Web-based administration allows you to easily configure and monitor your streaming server both locally and remotely.
- A relay allows you to set up a hierarchy of several layers of servers to broadcast streams to a virtually unlimited number of clients.

Viewing Streamed Media: How It Works

QuickTime Streaming Server streams can be viewed by both Macintosh and Windows users using QuickTime Player (which is available for free on Apple's Web site) or any other application that supports QuickTime. Streams can also be set up so that users can view them from within a Web browser when the QuickTime Plugin is installed.

When a user starts to play streamed media through a Web page, the QuickTime Plugin sends a request to the server.

When a user uses QuickTime Player to view multimedia on demand, the client computer sends a request for the server to play the multimedia file. The server looks for the hinted movie file, and if it's found, sends the media to the client computer.

When a user tunes in to a live broadcast, the QuickTime streaming client (for example, QuickTime Player) sends a request to the QuickTime Streaming Server. The server looks for a Session Description Protocol (SDP) file, and if it's found, begins to send the media to the client computer. An SDP file contains information about the format, timing, and authorship of the live broadcast. SDP files are created by broadcast software on the computer that captures the live media, but the SDP file must be copied to the streaming server before the media can be broadcast.

When a user tunes in to a prerecorded broadcast, a similar process happens: the server looks for an SDP file. In this case, an SDP file is created automatically when you start broadcasting playlists. If the SDP file isn't created on the streaming server, it must be copied to the streaming server before the prerecorded media can be broadcast.

Who Should Use QuickTime Streaming Server?

Anyone interested in delivering either audio or video over the Internet in real time should use QuickTime Streaming Server. For example, you can use QuickTime Streaming to

- create a 24-hour-a-day Internet radio station
- broadcast live events such as concerts, company meetings, and school assemblies
- create a distance-learning Web site, with video of lectures available on demand

Before You Set Up QuickTime Streaming Server

Before you set up QuickTime Streaming Server, be aware of the streaming server requirements listed here:

Client computer requirements

- Any computer that has QuickTime 4 or later installed can view media streamed by QuickTime Streaming Server. While not required, QuickTime 5 is recommended.

You can download QuickTime client software from the QuickTime Web site at www.apple.com/quicktime

Server requirements

- You can use the QuickTime Streaming Server software on a Power Mac G4, Macintosh Server G4, Power Mac G4 Cube, Power Macintosh G3, Macintosh Server G3, and iMac computers.
- The latest version of Mac OS X Server must be installed.
- You must have at least 128 megabytes (MB) of random-access memory (RAM). If you anticipate heavy traffic on your server, Apple recommends a minimum of 512 MB of RAM and 500 MHz or higher processor speed.

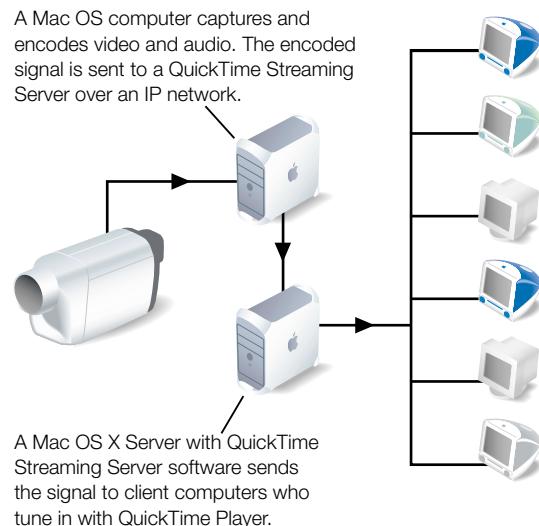
Live broadcasting requirements

You need the following equipment to stream live audio or video:

- Recording equipment for audio, video, or both
- A computer that has broadcast software and a video or audio capture card installed. You can also use a computer with a FireWire connection. You use this computer to capture and encode live audio or video and then broadcast it to your streaming server.

Sample Setup for Live Video

The illustration below shows a setup for streaming live video and audio. (Most video cameras have a built-in microphone.) You can stream audio only using a microphone, mixer, and other appropriate audio equipment.



Setting Up QuickTime Streaming Server for the First Time

To set up and manage QuickTime Streaming Server, you use the Web-based Streaming Server Admin program. You must use Streaming Server Admin from a computer capable of running Netscape Navigator, Netscape Communicator, or Microsoft Internet Explorer, versions 4.5 or later.

Step 1: Open Streaming Server Admin

To open Streaming Server Admin:

- 1** Open a Web browser.
- 2** Enter the URL for Streaming Server Admin on your server (make sure you add the colon and the port number, 1220).

For example:

`http://www.myserver.com:1220`

Replace “www.myserver.com” with the name of your server.

- 3** Type the streaming server administrator ID and password in the Login and Password text fields, then click Submit. The ID is “streamingadmin” and the default password is “default.” The Streaming Server Admin Web page appears and provides a quick snapshot of the server’s status. Click Status, Settings, or Logs at the top of the page to administer those areas.

Note: If QuickTime Streaming Server was properly installed, you can also open Streaming Server Admin from the Dock.

To get help when using Streaming Server Admin, click the question mark.

Step 2: Choose your streaming server settings

To change the settings for the streaming server:

- 1** Click Settings.
- 2** Click General Settings, Logging Settings, or Playlists Settings.
- 3** Make the changes you want and click Submit.

For more information on the available settings, see “Streaming Server Settings” on page 177.

Step 3: Set up a Web page to show streamed media (optional)

You can embed streamed media in a Web page. If you do this, viewers can use any Web browser to view the media by entering the URL of the Web page.

For example, users might enter this URL:

`http://www.mywebpage.com/`

In this case, “www.mywebpage.com” would be replaced by the DNS name of your Web site.

Setting Up a Web Page With Streamed Media

To embed streaming media in a Web page, you use the HTML EMBED tag. For complete documentation on the features and use of the EMBED tag, go to www.apple.com/quicktime/products

The following example code places a graphical link to a movie, “sample.mov,” on a Web page. (You can rename the Sample Movie that comes with QuickTime and use it for the example.) When a user clicks the link, the movie will start streaming in QuickTime Player.

```
<HTML>
<BODY>
This is a sample use of the EMBED tag.<BR>
<EMBED SRC="http://my.webserver.com/linkimage.mov" width="150"
height="64" href="rtsp://my.streamingserver.com/sample.mov"
target="QuickTimePlayer">
</BODY>
</HTML>
```

The URL specified in the `SRC` attribute is a link to a still image, “linkimage.mov,” that serves as the link to the streaming movie. The `width` and `height` attributes specify the width and height of the image area. The `HREF` attribute is the URL for the streaming movie that will start playing when the image is clicked.

You can also let users view streaming media from a Web page by creating a reference movie that contains a streaming track with an RTSP URL that points to the media on your streaming server. You store the reference movie in the same directory as your Web site and include a link to the reference movie on your Web page. For more information on creating a reference movie, go to developer.apple.com/quicktime/quicktimeintro/tools/index.html and look for the MakeRefMovie tool under “WebMaster Tools.”

A reference movie can simply be a text file with a “.mov” filename extension (such as “ref.mov”). The format for the contents of the file is as follows:

```
rtsp:text rtsp://my.streamingserver.com/sample.mov
```

Streaming Server Settings

General Settings

Movies Directory

Any hinted media in the movies directory you specify is available for streaming. This includes

- individual files
- directories that contain files
- links to media located elsewhere

The default location of the Movies Directory is /Library/QuickTimeStreaming/Movies/. You can select another directory on another volume.

Authentication Scheme

Choose between Basic or Digest. By default, the server uses the more secure Digest authentication. However, Digest authentication requires that users connect with QuickTime 5 or later. Basic authentication is less secure than Digest but is compatible with earlier versions of QuickTime.

Streaming on Port 80

Choose whether you want to serve QuickTime streams on HTTP port 80. If you need to serve streams past firewalls, you may need to enable streaming on port 80. Enabling HTTP streaming on port 80 does not prevent HTTP streaming on other ports. However, it can interfere with HTTP traffic on port 80 if you’re providing Web service on the same server (see “Streaming on Port 80” on page 188 for additional information).

Maximum Number of Connections

When the maximum number of connections is reached, users who try to connect see a message that the server is busy (error 453). Make sure you balance available bandwidth, the size of the media files being served, and the number of clients tuning in to the broadcast.

Maximum Throughput

This is the maximum throughput of the server. If the maximum throughput is reached, no one else can connect. Users who try to connect see a message that the server is busy (error 453). Keep in mind that the QuickTime Streaming Server may share throughput with other devices on your network.

Start Server at System Startup

This option restarts the streaming server each time your computer restarts.

Streaming Server Administrator’s Password

Enter the streaming server administrator’s login password. Confirm by entering the login password again on the next line. The default password is “default”; you can change it to whatever you like.

Logging Settings

Adjust these settings by changing information in the fields or clicking the preferred button. You can specify that the log be reset after a certain number of days or after it reaches a certain size in kilobytes (KB). The changes you make take effect when you click Submit.

Error Log

The error log shows error and informational messages. Use this to troubleshoot problems with the server. The complete error log can be found in /Library/QuickTimeStreaming/Logs/Error.log.

Access Log

The access log shows the number of times each media file has been accessed, when it was accessed, and who accessed it since the log was reset. Access errors are also reported in the log. The complete access log can be found in `/Library/QuickTimeStreaming/Logs/StreamingServer.log`.

Connected Users

In this pane, you can view a list of clients connected to your streaming server, and view additional information, such as the movie they’re watching and their IP address. You can display the information in a number of ways using the screen controls described below.

Number of entries to display

Choose a number from the pop-up menu to change the number of users displayed.

Update interval for this page

Choose a number from the pop-up menu to change how often the list is updated.

Selecting Sort Order

Choose either Ascending or Descending from the pop-up menu to select the sort order.

Selecting sort column

Click the column label by which you want to sort the list of connected users.

Streaming Server Strategies and Tips

Preparing Live Media for Streaming

To stream live audio or video, you need to do the following:

- 1** Set up your broadcast software following the instructions that came with it.
- 2** Connect the audio or video equipment to the computer you’re using to capture and encode the signal.
- 3** Use your broadcast software to create a Session Description Protocol (SDP) file on the computer you use to capture and encode the live signal.
See the instructions that came with your broadcast software.
- 4** Copy the SDP file to your QuickTime Streaming Server computer.
Be sure to copy the file into the directory you’re using for streaming.
- 5** If you want the streamed media to show on a Web page, set up the Web page by using the EMBED tag or creating a separate QuickTime reference movie (see “Setting Up a Web Page With Streamed Media” on page 176).

- 6** Make sure the streaming server is running.
- 7** Start the broadcast software following the instructions that came with it.
- 8** Tell users how to view the streamed media by providing them with an RTSP URL to your SDP file, or an HTTP URL to the QuickTime reference movie that you placed on your Web server.

Preparing Stored Media for Streaming

To prepare stored media for streaming:

Step 1: Add hint tracks to your media

Hint tracks contain information the streaming server needs to stream the media properly. Most authoring applications let you export media as a hinted QuickTime movie. If you have QuickTime Pro, you can also hint a movie using QuickTime Player. QuickTime Pro is available for both Mac OS and Windows computers. Check the QuickTime Web site for information on system requirements and installation instructions.

Each track in a media file must have its own hint track. For example, a movie with one audio and one video track must have two hint tracks: one for the audio track and one for the video track.

When you use QuickTime Player to export a movie as a hinted movie, QuickTime adds the appropriate number of hint tracks automatically.

To export a QuickTime movie as a hinted movie:

- 1** Open QuickTime Player on a Mac OS or Windows computer. (You must have QuickTime Pro to do this.)
- 2** Open the media file you want to hint.
- 3** Choose Export from the File menu.
- 4** Choose “Movie to Hinted Movie” from the pop-up menu, then type a new filename.
- 5** Click Options in the export dialog box.
- 6** Select Optimize Hints For Server. This is optional. It improves the server’s ability to stream to more clients but can double the size of the file.
- 7** Click OK.
- 8** Click Save.

Step 2: Copy the media file to your QuickTime Streaming Server

Be sure to copy the file into the directory you’re using for streaming.

Streaming Media Files With Multiple Sources

QuickTime movies often consist of content from several media files. For example, a video clip might be combined with music from one or more CD tracks. When you export a QuickTime movie, you should make it a “self-contained” file so that it includes all the source media. This improves server performance.

To stream movies that are not self-contained, in addition to hinting, you must

- copy all the files needed by the movie to the same folder or directory
- store all the files in the directory on your server that you specified as the Movies Directory in QuickTime Streaming Admin

Using Playlists to Broadcast Prerecorded Audio or Video

You can create a virtual “radio station” or video broadcast by setting prerecorded QuickTime media files to play in a specified order (*a playlist*). Setting up a series of playlists and clicking the Play button for each one broadcasts the media to the QuickTime Streaming Server, which sends the media to viewers in the sequence you set up (random or ordered). Although the media is prerecorded, it appears to viewers as a live broadcast. All viewers see the same media being played when they tune in to the broadcast.

To broadcast media, you need to do the following:

Step 1: Prepare QuickTime media and a reference movie file

You can broadcast any media that the QuickTime Streaming Server is capable of streaming.

To prepare the media:

- Use the same number of tracks and the same types of tracks for each movie in the playlist. Be sure all the media files contain compatible media types. For example, all audio tracks should use the same encoding, compression, and bit rate. All video tracks should also use the same encoding, compression, and bit rate.
- Format the media in each file in the same way. For example, use the same frame size for each file that contains a video track.
- Be sure each item is a hinted QuickTime movie.

To prepare a reference movie:

- Usually you specify the first media file in a playlist as the reference movie. However, you can author a separate reference movie.
- If you author a separate reference movie, it must be a hinted QuickTime movie that contains the same number of tracks, type of tracks, encoding, compression, and bit rate used in the actual media files.

Step 2: Create a playlist

To create playlists:

- 1** In Streaming Server Admin, click Settings, then click Playlists Settings.
- 2** Click Create New Playlist.
- 3** Enter a name for the playlist.
- 4** Use the pop-up menu to set a play mode:
 - *Sequential*: The media is broadcast in the order it appears in the playlist file. When the last media file is done playing, the broadcast stops.
 - *Sequential Looped*: The media is broadcast in the order it appears in the playlist file. When the last media file is done playing, the playlist repeats in the same order.
 - *Weighted Random*: The media is broadcast in random order using the weights you specify in step 7 to determine how often an item plays. The media continues to play in random order until you stop the broadcast.
- 5** If you want the server to record information about the broadcast (including error messages) in the log file, click Enable Logging.
- 6** Click Add/Remove Items to add movie files to your playlist.
- 7** Set the order and weight of your media files.

You can broadcast the media in the playlist sequentially or randomly, either once through the list or repeatedly through the list.

If you broadcast the media randomly, you can specify a “weight” for each media file in the list. The weight, which is a number from 1 to 10, determines how often an item plays. Media files that are weighted as 10 play more often than media files weighted with lower numbers. (You place the weight after the movie name.) The default weight for a media file is 10. In addition to using weights, you can prevent a media file from playing again until a specified number of other media files play.

- 8** Set the number of items that must play before other items in the list repeat (if weighted).
- 9** Click Submit to save your playlist.

Note: Hinted media files and playlists can be stored anywhere on your server, not just in the designated Movies Directory. Hinted media files stored outside of the movies directory can be broadcast as part of a playlist, but are not directly accessible by QuickTime clients.

Step 3: Start broadcast service

To start and stop broadcasts, return to the Playlists Settings pane in Streaming Server Admin. Click the Play button in the Controls column to start broadcasting a playlist, or click the Stop button to stop broadcasting a playlist.

Step 4: Tell users how to connect to the broadcast

To connect to the broadcast, users need software that can play QuickTime media, such as QuickTime Player.

For best results, users should have the latest version of the QuickTime software installed.

If you set up a Web page to show streamed media, users can connect to a broadcast using a Web browser that has the QuickTime Plugin installed. You need to provide users with the URL for the Web page and properly embed the link to play the media when clicked (see “Setting Up a Web Page With Streamed Media” on page 176).

If users tune in to the broadcast using QuickTime Player, you need to provide them with the URL for the SDP file that connects to the playlist broadcast.

Solving Problems With Playlists

If you enable logging, you can use the log file to troubleshoot problems that occur during the broadcast.

If the media in the playlist is not being broadcast:

- Check Streaming Server Admin to make sure the streaming server is running.
- If the streaming server is running, open ProcessViewer on the server computer and make sure a process called “PlaylistBroadcaster” is running. If it is and the media is not being broadcast, stop the broadcast, delete the SDP file for the broadcast from the QuickTime Streaming Server Movies Directory, then restart the broadcast. A new SDP file is generated when you restart the broadcast.

If the media in the playlist is not being broadcast randomly:

Make sure the Weighted Random play mode is specified.

If the media plays once and then stops:

Make sure the play mode is set to either Sequential Looped or Weighted Random.

If you broadcast the playlist as Weighted Random and set a value other than zero for repeated items, make sure the number is less than the number of media files in the playlist.

If some media in the playlist is not played:

Check the weight you have assigned to each media file in the playlist. If you change the playlist, you must stop and restart the broadcast for the changes to take effect.

If the media isn't streaming correctly:

Be sure the content, format, and encoding of the media is the same for all files in the playlist. Also, be sure users have the latest version of the QuickTime software installed on their computers.

If streaming is slow:

Be sure each media file is a hinted movie optimized for the server.

Inside QuickTime Streaming Server

Compatible File Formats

You can stream these media files using QuickTime Streaming Server for playback with QuickTime Player, as long as the media is hinted:

Category	Formats
Video	QuickTime AVI
Audio	AIFF/AIFC SoundDesigner II System 7 Sound μ Law (AU) WAV
MIDI	Karaoke MIDI Standard MIDI

Media files can be compressed using these methods:

Category	Compression-decompression method (codec)
Preferred video	Sorenson Video H.263 Motion JPEG A H.261
Supported video	Animation Cinepak Graphics Motion JPEG B MPEG-1 Photo JPEG Video None

Category	Compression-decompression method (codec)
Preferred audio	MP3 QDesign Music codec QUALCOMM Pure Voice DVI 4:1 ALaw 2:1 μ Law 2:1 16-bit raw
Supported audio	IMA 4:1 MACE 3:1 MACE 6:1

Controlling Access to Streamed Media

QuickTime Streaming Server comes with an authentication module, QTSSAccessModule, which you can use to control client access to streamed media files. Two schemes of authentication are supported: Basic and Digest. By default, the server uses the more secure Digest authentication.

The QTSSAccessModule, in addition to controlling access to streamed media, also lets you control playlist access and administrator access to your streaming server. It does not control access to media streamed from a relay server. Authentication for relayed media must be set up by the administrator of the relay server.

The QTSSAccessModule is built into QuickTime Streaming Server, so it is always enabled.

What Clients Need to Access Protected Media

Users must have QuickTime 5 or later to access a media file for which Digest authentication is enabled. If your QuickTime Streaming Server is set up to use Basic authentication, users need QuickTime 4.1 or later. Users must enter their user name and password to view the media file. Users who try to access a media file with an earlier version of QuickTime installed will see the error message “401: Unauthorized.”

Setting Up Access Control

For access control to work, an access file must be present in the directory you selected as your Movies Directory. If an access file is not present in the QuickTime Streaming Server Movies Directory, all clients are allowed access to the media in the directory.

To set up access control, you must do all of the following:

- create an access file
- create a user file
- add users to the file

You can also create a group file, but it's optional.

Step 1: Create an access file

An access file is a text file called “qtaccess” that contains information about users and groups who are authorized to view media in the directory in which the access file is stored. The directory you use to store streamed media can contain other directories, and each directory can have its own access file. When a user tries to view a media file, the server checks for an access file to see whether the user is authorized to view the media. The server first looks for an access file in the directory where the media file is located. If an access file is not found, it looks for it in the enclosing directory. The first access file that's found is used to determine whether the user is authorized to view the media file.

Note: The access file for QuickTime Streaming Server works similarly to the Apache Web server access file.

You can create an access file with any text editor. The filename must be qtaccess and the file must follow this format:

```
AuthName <message>
AuthUserFile <user filename>
AuthGroupFile <group filename>
require user <username1> <username2>
require group <groupname1> <groupname2>
```

Anything not in angled brackets is a keyword. Anything in angled brackets is information you supply.

- “Message” is text your users see when the login window appears. It's optional.
If your message contains any white space (such as a space character between terms), make sure you enclose the entire message in quotation marks.
- “User filename” is the path and filename of the user file. The default is /etc/streaming/qtusers.
- “Group filename” is the path and filename of the group file. The default is /etc/streaming/qtgroups. A group file is optional. If you have a lot of users you may find it easier to set up one or more groups, then enter the group names, rather than list each user.
- “Username” is a user who is authorized to log in and view the media file. The user's name must be in the user file you specified. You can also specify “valid-user,” which designates any valid user.

- “Groupname” is a group whose members are authorized to log in and view the media file. The group and its members must be listed in the group file you specified.

Additional user tags

This section describes additional tags you can add to the qtaccess file.

- “valid-user”
“Valid-user” is any user defined in the qtusers file.
The statement “require valid-user” specifies that any authenticated user in the qtusers file can be given access to the media files. If this tag is used, the server will prompt users to enter an appropriate user name and password to view the media.
- “any-user”
“Any-user” allows users to view media without being authenticated. If the statement “require any-user” is used, any user can have access; no name or password is required.

Step 2: Create a user file

To let users access your media files, you must add them to a user file.

To create a user file, open a terminal window and type the following:

```
qtpasswd -c <authentication realm> <user filename> <user-name>
```

“Authentication realm” is the message that is displayed to client users in the authentication window. For Basic authentication, if the “AuthName” keyword is used in the access file, users will see the realm listed in the access file; if the keyword is not present, users will see the realm from the user file. For Digest authentication, the “AuthName” keyword in the access file is ignored, and the authentication realm in the user file is always presented to client users. If you’re using Digest authentication, the realm cannot be changed once a user file is created. If it needs to be changed, the user file must be re-created.

You are asked to enter a password for the user. A file is created with the user you specified.

Note: The -c option creates a file. You use this option only once; if it is used for an existing file, you will be prompted before the file is overwritten.

Step 3: Add users to the user file

To add a user to the user file, open a terminal window and type the following:

```
qtpasswd <user filename> <user-name>
```

You’ll be asked to enter a password for the user. Re-enter the same password a second time when prompted.

Step 4: Add or delete groups

You can create a group file with any text editor as long as it follows this format:

```
<groupname>: <user-name1> <user-name2> <user-name3>
```

To add or delete a group, simply edit the group file you set up.

Making changes to the user or group file

To delete a user from a user or group file, do this:

- Use a text editor to open the user or group file. Delete the user name and encrypted passwords line from the user file; delete the user name from the group file.

To change a user password, do this:

- Open a terminal window and type the following:

```
qtpasswd <user filename> <user-name>
```

You'll be asked to enter a password for the user. The password you enter replaces the password that's in the file.

Getting Media Through Firewalls or Networks With Address Translation

QuickTime Streaming Server sends data using User Datagram Protocol (UDP) packets. Firewalls designed to protect information on a network often block UDP packets. Client computers located behind a firewall that blocks UDP packets can't receive streamed media. However, QuickTime Streaming Server also allows streaming over HTTP connections, which allows streamed media to be viewed through even very tightly configured firewalls.

Some client computers located on networks that use address translation may also be unable to receive UDP packets, but they can receive media that's streamed over HTTP connections.

If users are having problems viewing media through a firewall or via a network that uses address translation, they should upgrade their QuickTime software to the latest version. If users still have problems, their network administrator should provide them with the appropriate settings for the Streaming Proxy and Streaming Transport panes of the QuickTime Settings control panel.

Network administrators can also set their firewall software to permit RTP and RTSP throughput.

Streaming on Port 80

If you are setting up a streaming server on the Internet and you think some of your clients are behind firewalls that only allow Web traffic, you should enable streaming on port 80. Once you do so, the QuickTime Streaming Server accepts connections on port 80, the default port for Web traffic, and QuickTime clients will be able to connect to your streaming server even if they are behind a Web-only firewall.

Once you enable streaming on port 80, you can't run a Web server on the same computer as your streaming server unless you do one of the following:

- *Set up multiple IP addresses on your server:* These addresses can be on the same network interface card or on multiple interface cards. Configure your Web server and streaming server to accept connections on separate IP addresses.
- *Have your Web server accept connections on a port other than 80:* If you do this, you must change all URLs that point to the Web server to include the port number you have chosen.

Setting Up a Relay

Media streams are sent from a server to a client computer in one of two basic ways:

- *Unicast* is a one-to-one transmission. Each client computer that tunes in to a stream receives its own stream.
- A *multicast* stream is sent to a group address. This means several client computers can tune in to the same stream.

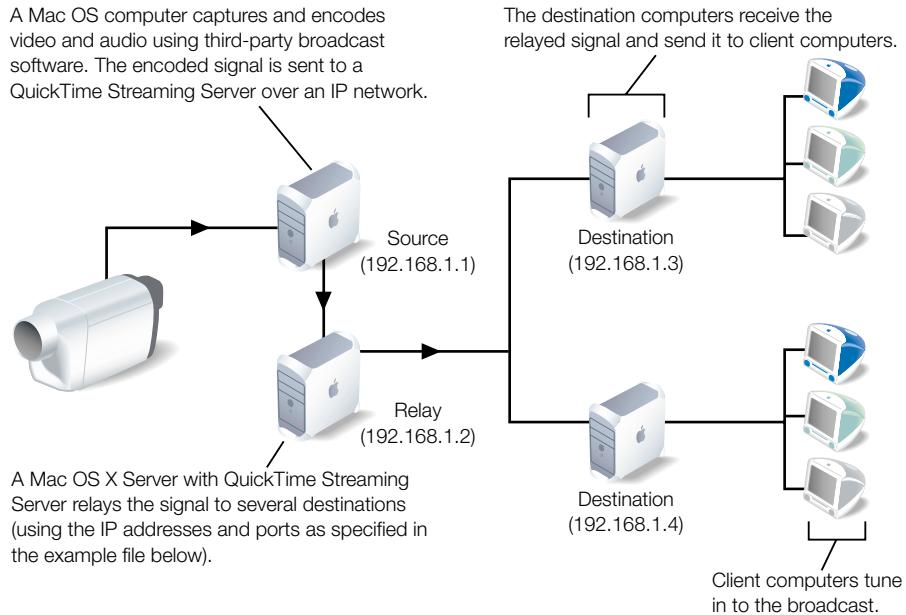
A relay listens to an incoming broadcast (either unicast or multicast) and forwards, or relays, that broadcast to one or more destination addresses (the broadcast can be relayed as either unicast or multicast as well). You can set up your server to relay multiple broadcasts at the same time. Relays take advantage of multicasting, or streaming data to multiple destinations at the same time. They're an efficient way to send high bandwidth data, such as multimedia, when you have a large number of users who want the same data.

A relay can be used to implement a large broadcast involving several tiers of streaming servers. For example, if you are expecting 3,000 clients to watch a live broadcast, and you want to use five different servers to handle the load, you can have your broadcasting application send the broadcast to a streaming server that acts as a relay. The relay can then forward one copy of the broadcast to each of the five streaming servers.

In addition, a relay can be used to take advantage of IP multicast. Multicast is an Internet technology that allows a single copy of a stream to be viewed by any number of clients, saving a lot of bandwidth. However, each router between the client and server must have IP multicast enabled, and multicast is disabled on some Internet routers.

If multicast is enabled on the network where your broadcast is taking place (a corporate or campus intranet, for example), a relay can be used to take an incoming unicast and relay it as a multicast. The resulting multicast can then be viewed by any client that "tunes in" to the stream. The relay can also be used to take an incoming multicast and relay it as a unicast. This is useful if multicast is not deployed over your entire network.

Sample setup for relaying a live broadcast



Setting Up a Relay Configuration File

You set up a relay by creating a relay configuration file and copying it to the /etc/streaming directory. The easiest way to create a relay configuration file is to edit the sample file provided with your streaming server software. The path and filename for the sample file is /etc/streaming/streamingrelay.conf

A relay source and one or more relay destinations are part of a unit. Information about a relay destination must immediately follow information about a relay source. You can have more than one unit in a configuration file.

The following example has one source and two destinations.

Important Although the relay_source and relay_destination lines are each split over two lines in the example, each must be on one line in your configuration file.

Example relay configuration file:

```
relay_source "in_addr=192.168.1.1 src_addr=192.168.1.2 in_ports=5000
              5002 5004 ttl=15"
relay_destination "dest_addr=192.168.1.3 out_addr=192.168.1.2
                  dest_ports=6980 6982 6984"
relay_destination "dest_addr=192.168.1.4 out_addr=192.168.1.2
                  dest_ports=10010 10012 10014 ttl=15"
```

These are the keywords and values that can appear in the relay configuration file.

Keyword	Value
relay_source	Followed by these keywords and an appropriate value for each keyword: in_addr, src_addr, in_ports, ttl
in_addr	Input IP address. If the source broadcast is a multicast, this is the multicast IP address. If the source broadcast is a unicast, this must be one of the IP addresses on the source computer.
src_addr	IP address of source (optional)
in_ports	Port number of the RTP streams in the source broadcast. These must be even numbers. The number of input ports should match the number of output ports; make sure port numbers are unique and don't overlap.
ttl	Time-to-live value (if it's a multicast source). A time-to-live value is used with multicasts to specify the number of times a media stream can be passed from one router to another before the stream is no longer transmitted. The value can be any number between 0 and 255. A value of 1 reaches client computers on the local area network. The larger the number, the farther the multicast packets will travel.
relay_destination	Followed by these keywords and an appropriate value for each keyword: dest_addr, out_addr, dest_ports, ttl
dest_addr	Destination IP address (unicast or multicast) of the relay
out_addr	IP address of the interface on which to send out multicast packets (optional). If not set explicitly, the output interface is chosen automatically.
dest_ports	Port numbers of the RTP streams in the destination relay. These must be even numbers. The number of output ports should match the number of input ports; make sure port numbers are unique and don't overlap. Use unassigned port numbers starting with 5000 and above.
include	Followed by a path and filename for a relay configuration file

If you enter a string that includes spaces in any configuration file, you must enclose the string in quotation marks. For example, “My Streaming Server” instead of My Streaming Server.

Turning a Relay On or Off

To turn off a relay, delete or rename the relay configuration file from the /etc/streaming directory. Then stop and restart the QuickTime Streaming Server.

To turn on a relay, create or copy a relay configuration file to the /etc/streaming directory. Then stop and restart the QuickTime Streaming Server.

Solving Problems With QuickTime Streaming Server

If Streaming Server Admin is not responding:

Verify that the streamingadminserver.pl script is running. If not, open the Terminal application (in /Applications/Utilities) and switch to the root administrator by typing “su root” and then the administrator password. Then start the Streaming Server Admin process by typing “streamingadminserver.pl” in the Terminal application.

If the server doesn't start up or quits unexpectedly:

- Check the error log.
- Make sure the QuickTimeStreamingServer file is in the /usr/local/sbin/ directory.

If the streaming server computer crashes or the streaming server computer is restarted:

- Once the computer has started up, you need to restart any playlists, even if Streaming Server Admin indicates they are playing.
- Make sure the QuickTimeStreaming Server is running *before* you restart the playlists.

If media files do not stream properly:

- Check the error log.
- Make sure the movie file is supported by QuickTime Streaming Server. Check the list of compatible file formats on page 184.
- Try streaming a sample movie to see if the server can stream it. A sample movie is included with the server.

If the server streams the sample movie, the problem may be with the way your movie file is prepared. Re-create the movie.

If the sample movie doesn't stream, the problem may be with the server computer or the network.

- Try hinting the movie again with the Optimize Hints For Server option selected.
- Check streaming server activity and, if necessary, reduce the maximum number of connections or throughput.
- If the problem occurs on a Mac OS client computer, open the TCP/IP control panel on the client computer and make sure MacIP is not selected.
- If the problem occurs on a client computer, make sure the user has the appropriate settings in the Streaming Proxy and Streaming Transport panes of the QuickTime Settings control panel. The administrator for the client computer's network should be able to provide the correct settings.
- If you are reflecting more than one live stream, make sure each stream uses a separate UDP port. Otherwise, client computers will show a message with error 500. You set up ports in the relay configuration file.
- Make sure the client software supports the file format being broadcast.
- Check the structure of the URL.

If streaming service is slow:

- If you are streaming QuickTime movies, make the movies self-contained using your authoring application, and make sure hinting is optimized for streaming services.
- Reduce the maximum number of connections or the throughput.
- Turn off other services.
- Place media files on other hard disks to improve server performance.

Because QuickTime Streaming Server can use only one Movies Directory, you need to create links from the Movies Directory you selected in Streaming Server Admin to the media files on other hard disks. To do so:

- On the computer where QuickTime Streaming Server is running, press the Control key and drag the folders that contain the media from the other disks to the folder you selected as the Movies Directory.

If users can't see the live streamed media:

- Make sure you are capturing a signal from the audio or video equipment into the computer you're using for capture and encoding.
- Make sure the SDP file is located in the Movies Directory on your streaming server.

Where to Find More Information About QuickTime Streaming Server

For more information about QuickTime Streaming Server, see these resources:

- QuickTime Streaming Server Web site
www.apple.com/quicktime/products/qtss/
- IP Multicast Initiative Web site
www.ipmulticast.com
- Email discussion list
lists.apple.com

QuickTime Streaming Server developers should look for the Streaming-Server-Developers list.

QuickTime Streaming Server users should look for the Streaming-Server-Users list.

Macintosh Management Service

What Is Macintosh Management Service?

Macintosh Management service lets you set network-wide policies for controlling user access to applications, file server volumes, and printers. You can also define the environment users see when they log in. Macintosh Manager is particularly useful for providing authentication and preference management for NetBoot client computers.

Who Should Use Macintosh Management Service?

You should consider using Macintosh Management service if

- you'd like to reduce the cost of managing a network of Macintosh computers
- you want to provide users with a consistent, controlled interface while allowing them to access their documents from any computer
- you need to secure computer usage in key areas such as administrative offices, classrooms, or open labs

Example: Using Macintosh Manager to Control Access to Computers

Let's say you've just purchased a number of new Macintosh computers for creating and editing movies. Due to space constraints, you've had to put the new computers in an open lab alongside other, general-use computers. You can use Macintosh Manager to reserve the new computers exclusively for users who must do video production work. To do so, you'd assign specific users to a "video production" workgroup, create a special "list" of video production computers, and give only the video production workgroup access to those computers.

Before You Set Up Macintosh Manager

Before you set up Macintosh Manager, be aware of the system requirements listed here:

Client computer requirements

- Mac OS 8.1 to Mac OS 9.x
- at least 1 megabyte (MB) of available random-access memory (RAM)
- 16-bit monitor recommended if using the Panels environment

Administration computer requirements

- Mac OS 9 or later, and Mac OS X
- at least 2 MB of available RAM
- minimum monitor resolution of 800 x 600

Setting Up Macintosh Manager for the First Time

To do the basic initial setup of Macintosh Manager, follow these steps:

Step 1: Make sure users with home directories exist in Users & Groups

Any user imported into Macintosh Manager must first exist in the Mac OS X Server Users & Groups database. Each user you plan to import must also have a home directory. See “Setting Up Users and Groups for the First Time” on page 59 for further information.

Step 2: Make sure Macintosh Management service is running

Use the Macintosh Mgr module of Server Admin to make sure the service is running. If the service is running, a globe appears on the service icon and the first menu item is Stop Macintosh Management Service. If the menu item is Start Macintosh Management Service, choose it to start Macintosh Manager.

Step 3: Log in as an administrator

Open Macintosh Manager by using the Macintosh Mgr module of Server Admin or by clicking the Macintosh Manager icon in the Dock. Log in to the server using a Mac OS X Server administrator account. (Later on, you can log in using this account or other administrator accounts that you set up.)

Step 4: Add user accounts

In the Macintosh Manager Users pane, you import users from Mac OS X Server. Required user information, such as name and email address, is imported into Macintosh Manager along with the user account. If you don't want to import users right now, you can set up the All Other Users account and grant immediate access to users with Mac OS X Server names and passwords (see "Providing Quick Access to Unimported Users" on page 228). Once you've added a user, you can also set options specific to Macintosh Manager (such as the user type, workgroup memberships, and so on).

Step 5: Create a Macintosh Manager administrator

You need to create at least one Macintosh Manager administrator account to keep other users from bypassing security. Macintosh Manager administrators can manage any of the Macintosh Manager settings and can use their passwords to log in as any other user (except as another Macintosh Manager administrator).

You can also set up workgroup administrator accounts for other people (such as teachers or technical coordinators) who need the authority to add or modify user accounts or workgroups. They also have access to hand-in folders. Workgroup administrators can use whatever Macintosh Manager features the Macintosh Manager administrator gives them access to.

Step 6: Create a workgroup

You need to create at least one workgroup of users. Workgroups let you group users according to privileges and shared resources, such as software, printers, and computers. For example, you may want to create one workgroup for specific types of users, and another for users who need to use a specific printer for a project.

Users can't log in to the Macintosh Manager network until they are assigned to a workgroup. (A user can belong to more than one workgroup.)

See "Creating Workgroups to Meet Your Network's Needs" on page 229 for more information.

Step 7: Set security options

You need to set some security options in the Global pane to safeguard information and control access to your network.

If your network includes any pre-Mac OS 9 client computers, use the Security pane of the Global pane to specify how user preferences (such as a desktop picture or Web browser preferences and favorites) are treated and stored for pre-Mac OS 9 client users. Choose one of the following:

- *Copy entire Preferences folder:* All items in the user's Preferences folder are copied from the server at login and to the server at logout, regardless of what the item is or how large it is. Be aware that copying unnecessary or large items may increase login and logout times.

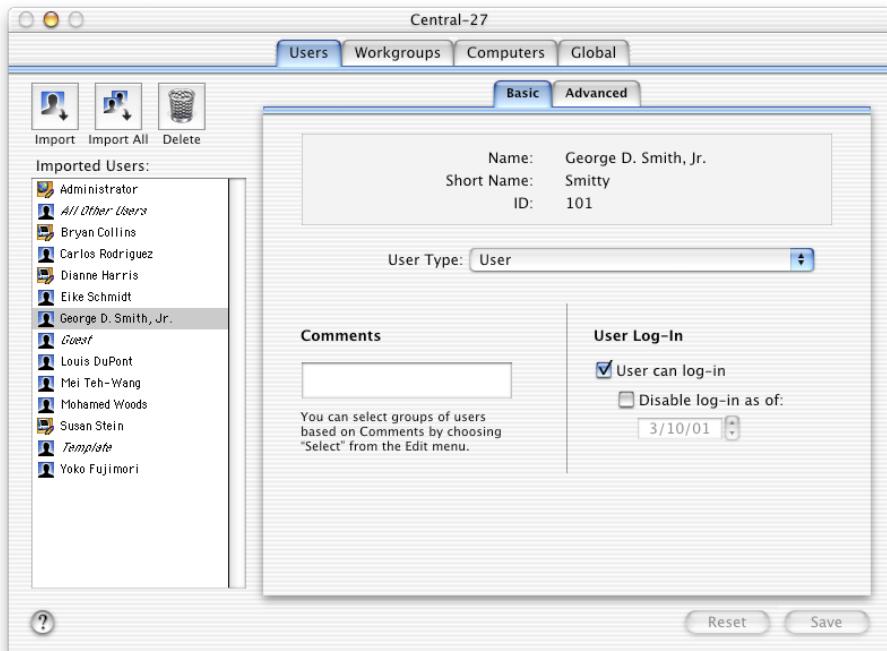
- *Copy only Internet or administrator-defined preferences:* If you are using managed preferences, any preferences in the Preserved Preferences folder are copied (see “How Macintosh Manager Works With Preferences” on page 232). If you are not using managed preferences, the following files and folders are copied from the server when the user logs in: StuffIt Expander Preferences, RealAudio™ Player Preferences, Internet Preferences, NCSA Telnet Preferences, Fetch Prefs, NewsWatcher Prefs, JPEGView Preferences, Netscape f, and Explorer (the cache folder inside the Netscape f and Explorer folders is deleted).

Macintosh Manager Settings

To access Macintosh Management service settings, open Macintosh Manager, log in to the server, and click the tab for the settings you want to change.

Basic Settings for Users

The Basic pane of the Users pane lets you set basic options for Macintosh Manager users.



Name, Short Name, and ID

These elements are imported from the Users & Groups database and can't be changed here.

“Short name” is the user’s short name, which you set in the Server Admin application. Users can use this instead of their full user name to log in to Macintosh Manager and other network services. If a user doesn’t have an email address, Macintosh Manager can assign an address based on the user’s short name and a domain you specify in the Control pane of the Computers pane.

User Type

The User Type pop-up menu lets you assign users one of three types of user accounts:

- *User accounts* are for people (usually students or employees) who use a computer for their daily work. This type of user has no privileges to use the Macintosh Manager administration application.
- *Workgroup Administrator accounts* are for people (usually teachers or managers) who need the authority to add or modify user accounts and/or workgroups. A Macintosh Manager administrator decides which features of Macintosh Manager the workgroup administrator can use. A workgroup administrator must be a member of each workgroup he or she manages.
- *Macintosh Manager Administrator accounts* are for people who manage the network and who need to set options that affect all users and workgroups. A Macintosh Manager administrator can use all the features available in Macintosh Manager. This is the only type of user who can set up a workgroup administrator or Macintosh Manager administrator account.

You must assign each user and workgroup administrator to a workgroup; otherwise the user cannot log in.

Comments

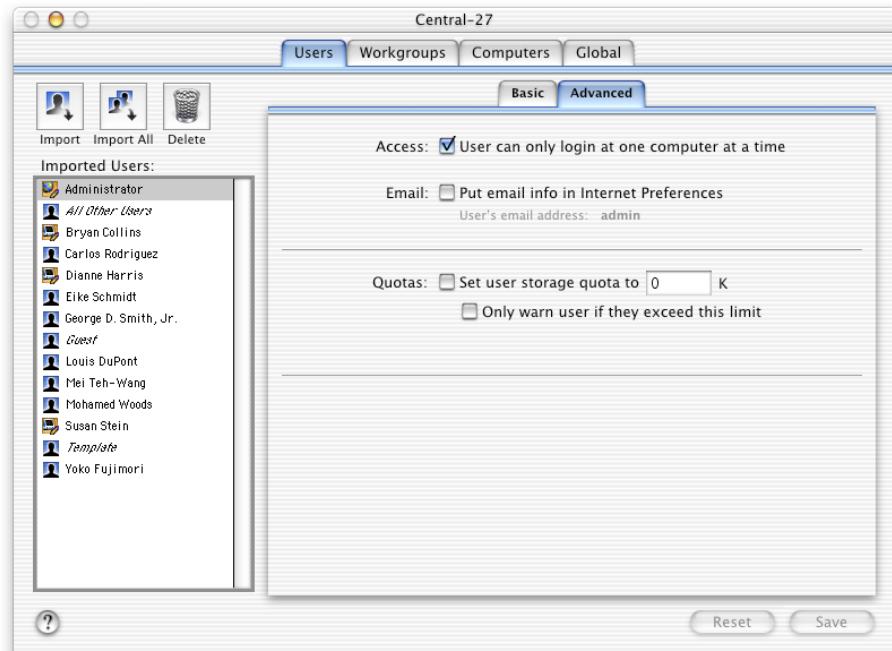
Enter any information (up to 63 characters) to help identify the user.

User Log-In

- Select “User can log-in” to let the user log in to any computer administered with Macintosh Manager. You can remove a user account immediately by disabling this setting.
- Select “Disable log-in as of” to disable user accounts in Macintosh Manager on a specific date.

Advanced Settings for Users

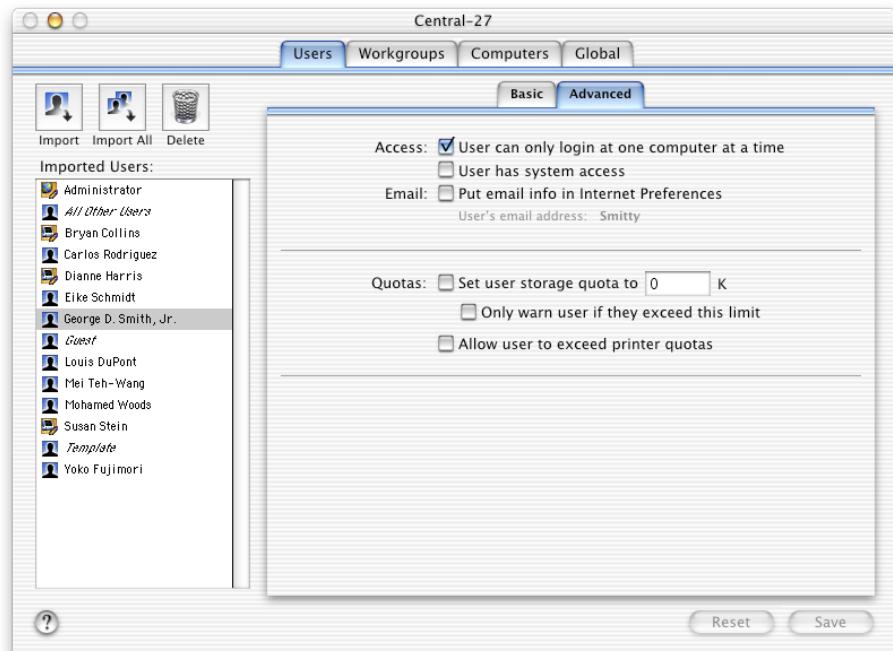
The Advanced pane of the Users pane lets you set advanced options for Macintosh Manager users. Different options appear depending on the user type (set in the Basic pane).



Advanced pane for a Macintosh Manager administrator

Access

- Select “User can only login at one computer at a time” to allow a user to log in to only one of the computers connected to this Macintosh Management server at a time. Users with this restriction must log out of the computer they are using before they can log in to or check out another.



Advanced pane for a User

- Select “User has system access” to allow a user access to all items on the client computer, including the Finder and the System Folder. When a user with system access logs in to a client computer, System Access appears as a choice in the login dialog. A Macintosh Manager administrator always has system access.

Email

Select “Put email info in Internet Preferences” to let Macintosh Manager check the mail server for messages when a user logs in. The user must have a Post Office Protocol (POP) or IMAP email account. When you first import users into Macintosh Manager, each user’s email account name and mail server data are imported from the Mac OS X Server user database, along with other user data. If email information does not already exist for a user in the Mac OS X Server database, you can enter mail server data in the Control pane of the Computers pane.

To set up Macintosh Manager to check for email automatically, you need to enable checking for email at login in the Options pane of the Workgroups pane, and the user needs access to email software.

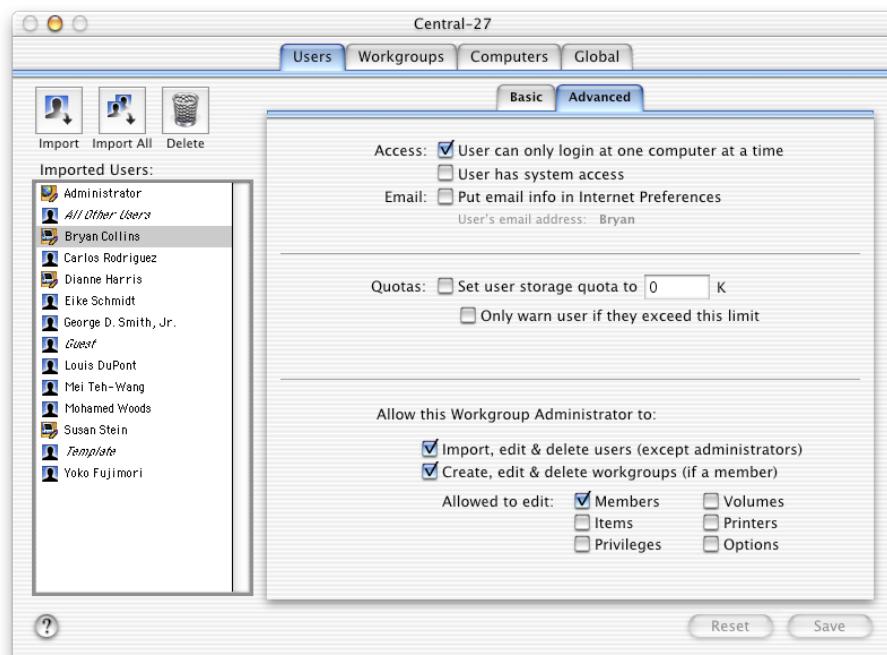
Quotas

- Select “Set user storage quota to _ K” and enter a value in the field to limit the amount of disk space users can take up in their home directory. Select “Only warn user if they exceed this limit” to have Macintosh Manager warn users when they’ve exceeded the limit. This does not prevent users from saving additional documents.
- Select “Allow user to exceed printer quotas” to let the user exceed the printer quota set in the Printers pane of the Workgroups pane.

Note: “Allow user to exceed printer quotas” is the only item that appears in the Advanced pane when All Other Users is selected.

Allow this Workgroup Administrator to

Select “Import, edit & delete users (except administrators)” and “Create, edit & delete workgroups (if a member)” to let the user perform those tasks. These settings appear only if the user is a workgroup administrator.



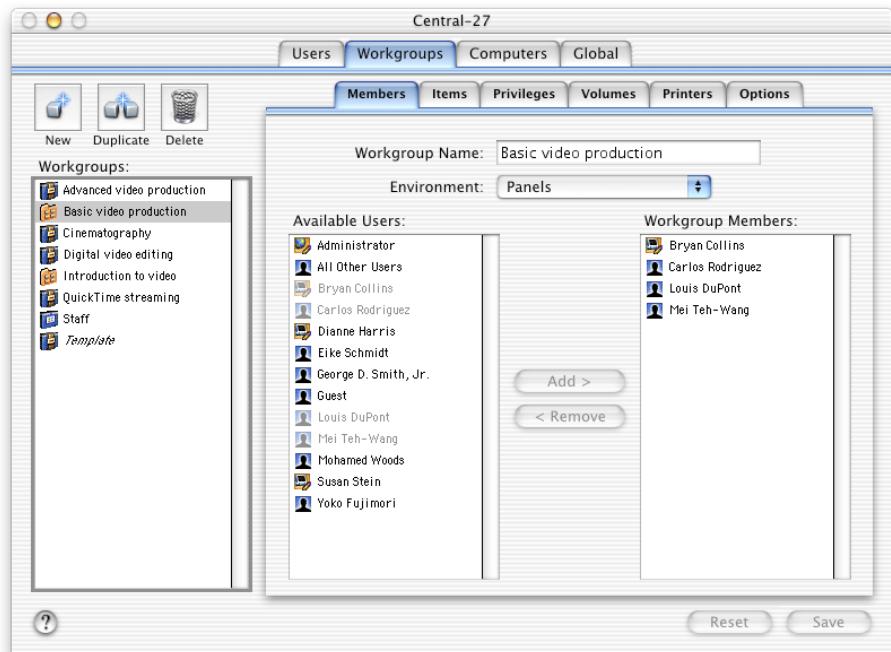
Advanced pane for a workgroup

Allowed to edit

If you let the user create, edit, and delete workgroups, select the workgroup settings panes you want the workgroup administrator to be able to modify. For example, you might select only the Members option if you want the user to be able to add or delete users from a workgroup, but not change any other settings for the workgroup.

Members Settings for Workgroups

The Members pane of the Workgroups pane lets you choose an environment and add members to your workgroups. Every user or workgroup administrator must be assigned to at least one workgroup to be able to log in. A user can be a member of up to 42 workgroups.



Workgroup Name

A workgroup name can contain most keyboard characters (including the period, underscore, dash, and space) except a colon (:) and can contain no more than 31 characters.

Environment

The Environment determines the interface users in a workgroup see, and the type of access workgroup members have to network resources. You can set up three types of environments:

- *Finder* is the standard Mac OS desktop. Few restrictions are imposed on users.
- *Restricted Finder* looks like the standard Mac OS desktop, but it protects workstations from tampering by restricting what users can do.
- *Panels* provides a simple interface with large icons that make using a computer easy for novice users, particularly children. The Panels environment provides the maximum amount of security because users do not have direct access to the startup volume. If you allow access to server volumes or removable media, each volume or media item appears as a panel when it is mounted. You can specify the names of workgroup and user documents panels in the Log-In pane of the Computers pane.

Available Users

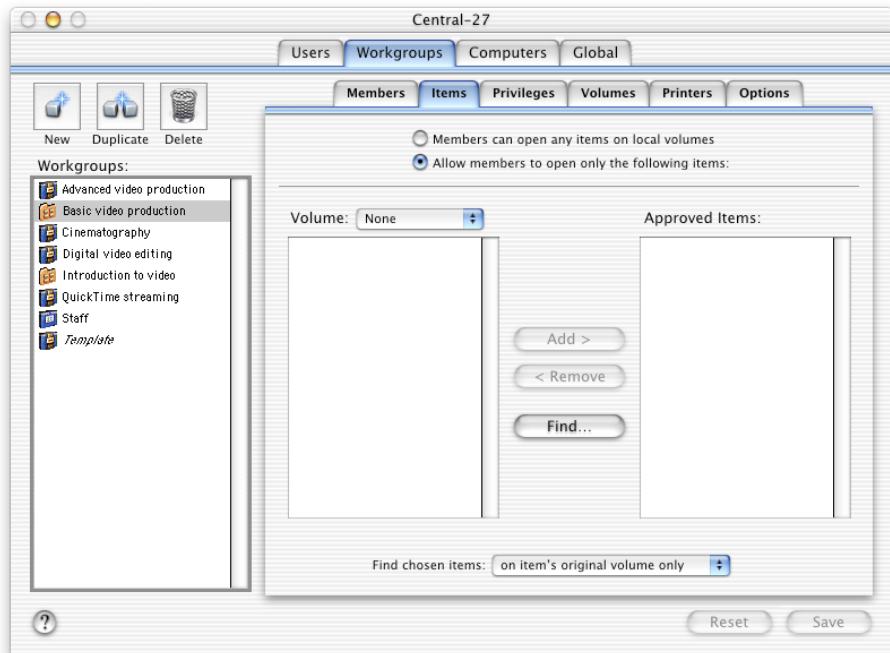
This list shows the names of all imported Macintosh Manager users, including the All Other Users account. Click a user in the list and click Add to add the user to a workgroup. You can also click and drag a user from this list into the Workgroup Members list.

Workgroup Members

Workgroup members can be of any user type: user, workgroup administrator, or Macintosh Manager administrator. A workgroup can have up to 1500 members. Select a user in the list and click Remove to remove the user from the workgroup.

Items Settings for Workgroups

The Items pane of the Workgroups pane lets you make files and applications on client computers available to workgroup members.



Members can open any items on local volumes

Select this option to allow members to open any files on local volumes. If you select this option, you can also set up the Shortcut Items list to give workgroup members quick access to a set of applications.

Allow members to open only the following items

Select this option to restrict workgroup members to just the items you select. If you select this option, you need to set up the list of approved items below.

Volume

If you're setting up a list of shortcut items or approved items, choose the volume where the items are located from the Volume pop-up menu. The items on the volume you choose appear in the field below. Locate and select an item, then drag it or click Add to add it to the list on the right.

Shortcut Items

This list appears if you are allowing workgroup members to open any items or if this is a Finder workgroup. Add items to the list to give members quick access to these items. Those items appear together in a folder for Restricted Finder workgroups and on a panel for Panels workgroups. Setting up a shortcut items list is optional.

Note: For the Finder environment, only the Shortcut Items list appears. If you add items to the list, these items appear as aliases on the user's desktop.

Approved Items

This list appears if you allow workgroup members to open only the item you select. You must add any items you want users to be able to access to the Approved Items list. Those items appear together in a folder for Restricted Finder workgroups and on a panel for Panels workgroups.

Find chosen items

When you make an application or document an approved item, the item is stored as an alias to the original application or document. When a user logs in, the computer locates the original file for each approved item and then downloads an alias to the client computer.

You can decide where the computer looks for workgroup items by selecting one of the following from the "Find chosen items" pop-up menu:

- "on item's original volume only" looks for the item on the volume where it originally resided (either a server volume or a local volume). The computer can only look on volumes that are mounted.
- "on local volumes first" looks on the local volumes available to a client computer. If the item is not found, and if the original item was on a server, then the computer looks on any mounted volumes.
- "on workgroup server volumes first" looks on the volume that stores the workgroup. If the item is not found, the computer looks for the item on the startup volume and other local volumes.
- "only on local volumes" looks for the item on locally mounted volumes, including the startup volume, additional partitions, and directly connected hard disks.
- "only on workgroup server volumes" directs the computer to look for the item on any Apple Filing Protocol (AFP) volume mounted for that workgroup. If the item is not found on one of these volumes, it cannot be opened.

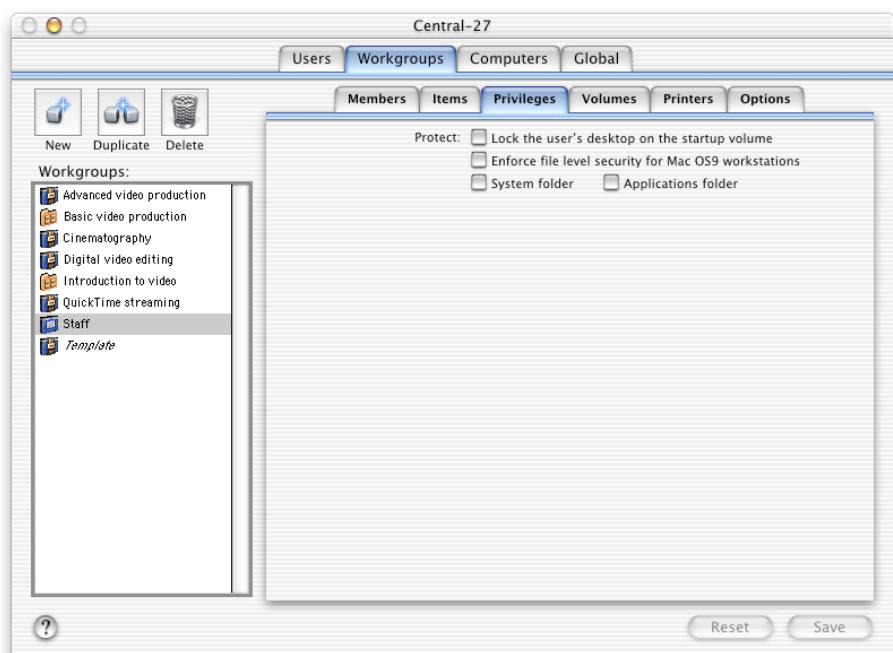
Keep in mind that for a NetBoot client computer, a local volume is the hard disk in the computer or any external hard disk connected directly to the computer. The startup volume for a NetBoot client computer is a remote volume, but it is treated as a local volume.

Important If you approve items for workstations while using the Macintosh Manager application on a computer where personal file sharing is turned on, or where any AFP file service is running, you may experience unexpected results. If you have trouble, use Macintosh Manager on a computer that does not have the file service installed on it. If you are approving all items with “only on local volumes” as the “Find chosen items” criteria, you can use Macintosh Manager while on the same computer where the file service is running without unexpected results.

Privileges Settings for Workgroups

The Privileges pane of the Workgroups pane lets you select various privileges settings for each workgroup.

The privileges you can set for a workgroup depend on the workgroup’s desktop environment. You cannot restrict most privileges for Finder workgroups, but there are a number of options you can set for the Panels and Restricted Finder workgroups.

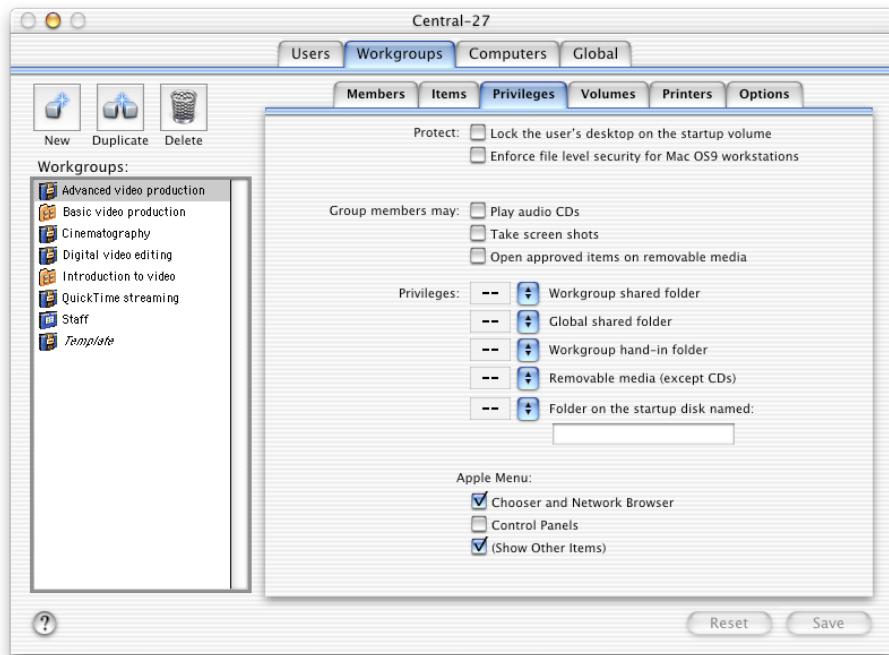


Privileges pane for a Finder workgroup

Protect

You can enhance workstation security by controlling whether applications can make changes to specific areas on client computers.

- Select “Lock the user’s desktop on the startup volume” to prevent the user or applications from changing or writing to the desktop.
- Select “Enforce file level security for Mac OS 9 workstations” to provide strict security. Enforcing file level security prevents applications from writing to restricted areas, but it may cause some older applications not to launch properly or to report disk errors. If you don’t enforce file level security, applications can write information wherever they need to.
- Select “System Folder” and “Applications folder” to protect the System Folder, the Applications folder, or both (for Finder workgroups). The Applications folder must already be created and must be located at the top level of the startup disk.



Privileges pane for a Restricted Finder workgroup

Group members may

- Select “Play audio CDs” to let Panels and Restricted Finder workgroup members play audio CDs at the computer. An audio compact disc is a CD whose first track contains audio data. The client computer can’t distinguish one audio CD from another one, so you allow access either to all audio CDs or to none.

- Select “Take screen shots” to let Panels and Restricted Finder workgroup members take screen shots. Screen shots are saved automatically in the user’s documents folder. If disk space is a concern, you should prevent users from taking screen shots.
- Select “Open approved items on removable media” to let Panels and Restricted Finder workgroup members open any applications on removable media (other than CDs). You can set options for CDs and DVDs in the CD-ROMs pane of the Global pane. Be aware that allowing users to open approved applications on removable media may make client computers vulnerable to viruses. Unless you can screen removable media before it’s used, you should leave this setting disabled to help protect the computer from viruses.

Privileges

You can choose Read only, Write only, Read & Write, or no privileges for the following locations:

- *Workgroup shared folder*: If you select a workgroup data volume in the Options pane, this folder is created for the workgroup. Only members of the workgroup can use it.
- *Global shared folder*: If you select a workgroup data volume in the Options pane, this folder is created. Members of all workgroups whose workgroup folder is on the same volume can access the folder.
- *Workgroup hand-in folder*: If you select a workgroup data volume in the Options pane, you can set up a hand in folder for the workgroup. At least one workgroup administrator or Macintosh Manager administrator must be a member of the workgroup to use this feature. The administrator is the only one who can see the folder. Workgroup members put items into the folder by choosing Hand In from the File menu in the Panels environment or by dragging the item to the Hand In folder in the Restricted Finder environment.
- *Removable media (except CDs)*: This includes floppy disks, Zip disks, and all other types of removable media except CDs. You set options for CDs and DVDs in the CD-ROMs pane of the Global pane.

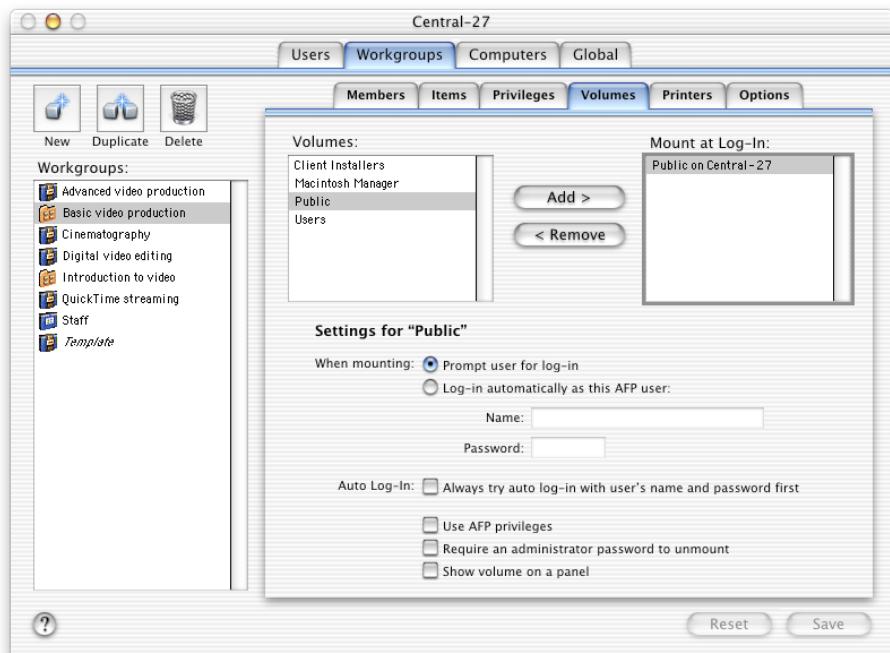
- *Folder on the startup disk named:* The Macintosh Manager administrator can create two types of folders on the startup disk of the client computer, each for a particular use. The first type is a standard folder with any name you like (such as Scratch) that can be designated as Read only or Read & Write. This type of folder can be used for storing clip art, or as the download folder for a Web browser. It can also be used as the preferred location for video and audio capture applications to store working files, so that these files don't need to be stored on and copied from remote volumes. The second type of folder lets you grant special permissions to the folder's contents by giving the folder a name that starts with the Option-8 bullet character (such as •Special Apps). As long as the folder name starts with a bullet, users can open any application inside the folder, regardless of whether the application is on the approved items list for the user's workgroup. For example, in an advanced graphics lab, a few of the computers may have Final Cut Pro installed instead of iMovie. Rather than creating another workgroup just for these few computers, the administrator can create the special folder on the computers, name it with the bullet symbol, and place Final Cut Pro inside. Users in that workgroup on other computers will see an empty folder that they can use for storage space. Users on the computers with Final Cut Pro installed inside the special folder can open Final Cut Pro on only those computers. This feature works for both Restricted Finder and Panels workgroups. Be extremely careful when using a special folder. Any application copied into that folder can be opened. Therefore, if there are applications on a local hard disk that should not be opened, they must be removed from the computer.

Apple Menu

Select each item—Chooser and Network Browser, Control Panels, and (Show Other Items)—you want members of the workgroup to see in the Apple menu (for Panels and Restricted Finder workgroups). For Panels workgroups, you can also restrict which items appear in the File and Special menus. Checked items appear in the menu. For all three types of workgroups, certain control panels are always off limits. These control panels are AppleTalk, Date & Time, Extensions Manager, File Sharing, Keychain Access, Location Manager, Multiple Users, Startup Disk, and TCP/IP.

Volumes Settings for Workgroups

The Volumes pane of the Workgroups pane lets you select various volume settings for each workgroup.



Volumes

This list shows all available volumes. This includes any share points set up using Server Admin. If you want a volume to be mounted when workgroup members log in, select the volume and drag it to the list on the right or click Add.

Mount at Log-In

This list shows all volumes you've selected to mount when workgroup users log in to client computers. To remove a volume from the list, select it and click Remove.

When mounting

When the volume is mounted, it will request a login name and password. You can select one of these options for providing the needed information:

- Select “Prompt user for log-in” if you are mounting a volume that doesn’t use the same user names and passwords used by Macintosh Manager. Users must enter a valid name and password for the volume.
- Select “Log-in automatically as this AFP user” to allow all users to log in with the same user name. It’s not as secure as requiring a user to log in with his or her user name, because you can’t control access individually and you can’t track who has logged in to the server.

Always try automatic log-in with user’s name and password first

When this option is selected, anything else you select as a mounting option is used only if automatic login fails. If you do not select automatic login, then the mounting option you select is the only option that’s used.

Use AFP privileges

Select this option to control volume access using the already established Apple Filing Protocol (AFP) privileges. This option is only available for Panels and Restricted Finder environments.

Require an administrator password to unmount

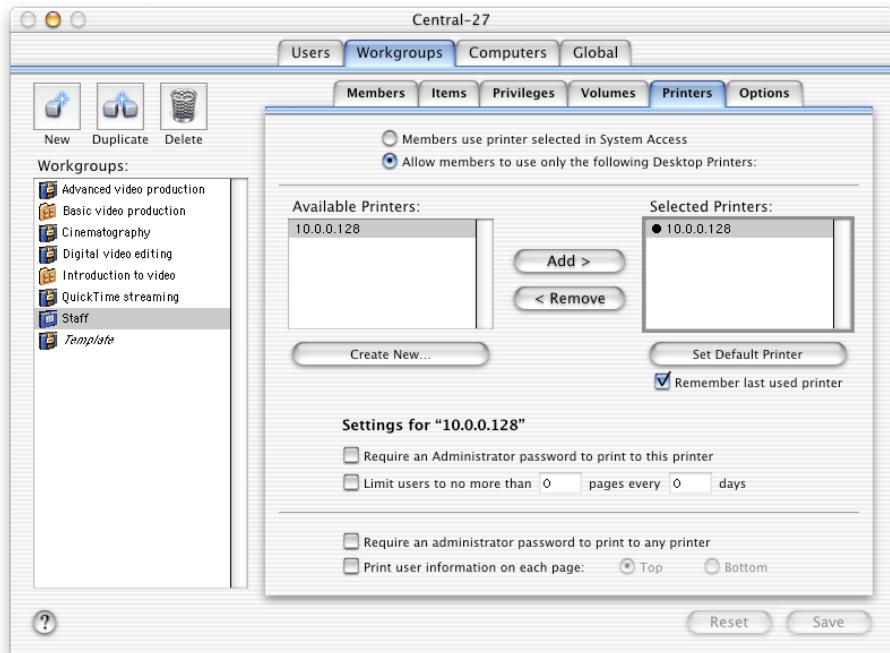
Select this option to require a workgroup administrator or Macintosh Manager administrator password to unmount the volume.

Show volume on a panel

Select this option to make the volume appear on a panel in the Panels environment.

Printers Settings for Workgroups

The Printers pane of the Workgroups pane lets you select printing options for each workgroup.



Members use printer selected in System Access

Select this option to require users to print to the printer that was assigned to their client computer as the default printer, either by a user logged in using the System Access workgroup, or by another user before Macintosh Manager was activated. The printer can be a desktop printer but does not have to be. If a desired printer does not support desktop printing, you must use this option to allow users to print to it.

To set up a System Access printer, an administrator must log in to each client computer using the System Access workgroup and use the Chooser to select a printer. If you specify that a workgroup should use the System Access printer, but do not select a printer from a client computer, users who log in to that computer will not be able to print unless they have access to the Chooser. Users who can see the Chooser can select from the printers visible to them. When using Macintosh Manager on Mac OS X, you can only select PostScript™-compatible printers as System Access printers.

When the user logs out of a client computer, the printer originally chosen by the administrator as the System Access printer becomes the default printer again.

Allow members to use only the following Desktop Printers

Select this option to make one or more desktop printers available to a workgroup. Drag each printer from the Available Printers list to the Selected Printers list, then click the printer you want to work with and adjust its settings. In order for desktop printers to work correctly in Macintosh Manager, the printers must be set up on each client computer by a user logged in using the System Access workgroup. Printers that were not already set up in System Access may not be available, or may not perform reliably.

Available Printers

This list shows all desktop printers that you can make available to the workgroup. To add a printer to the Selected Printers list, select it and click Add. If you don't see the desktop printer you want, you can set it up by clicking Create New.

Selected Printers

This list shows all the desktop printers you've made available to the workgroup. If you want to make a printer the default printer for the workgroup, select it and click Set Default Printer.

Require an Administrator password to print to this printer

Select this option to require a workgroup administrator or Macintosh Manager administrator password to use the selected desktop printer. Never give users your administrator password. To ensure the security of your own administrator account, you can set up a workgroup administrator account with no administration privileges and use the password for that account for printing.

Limit users to no more than _ pages every _ days

Select this option and enter a number of pages and days to limit workgroup members to the number of printed pages per number of days that you specify. You can override the quota for an individual user in the Advanced pane of the Users pane. You can only set printing quotas for desktop printers.

The number of pages refers to the document's page count, not the number of pieces of paper. If a user prints two pages per sheet of paper, the number of pages is twice the number of sheets of paper. Pages are counted whether or not the printing job completes properly (for example, if there is a paper jam).

Require an administrator password to print to any printer

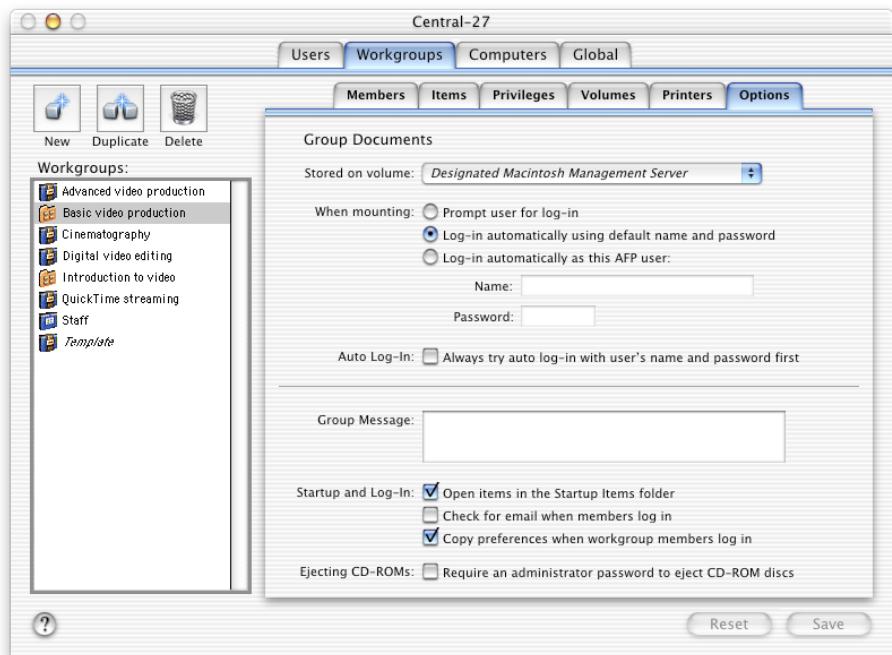
Select this option to require a workgroup administrator or Macintosh Manager administrator password to use any desktop printer, or only a specific printer. Never give users your administrator password. To ensure the security of your own administrator account, you can set up a workgroup administrator account with no administration privileges and use the password for that account for printing.

Print user information on each page

Select this option to print the user name, workgroup name, and time of printing at the top or bottom of each page. The information may overwrite other information on the page.

Options Settings for Workgroups

The Options pane of the Workgroups pane lets you select various settings for each workgroup, including the shared group document volume and what events should happen at login.



Stored on volume

Choose a volume where the workgroup can save and access shared documents. This volume is called the *workgroup shared volume* or *workgroup data volume*.

When mounting

Choose how users log in to the workgroup data volume:

- “Prompt user for log-in” forces users to enter a valid name and password for the volume. This setting is useful if you are mounting a volume that doesn’t use the same user names and passwords imported from the Mac OS X Server database.
- “Log-in automatically using default name and password” is available only if you choose Designated Macintosh Management Server as the workgroup volume. If this option is selected, the computer tries to log in to the workgroup volume with a generic user name and password. The generic user is set up automatically. It’s not as secure as requiring a user to log in with his or her user name, because you can’t control access individually and you can’t track who has logged in to the server.

- “Log-in automatically as this AFP user” logs all users in with the same user name. It’s not as secure as requiring a user to log in with his or her user name, because you can’t control access individually and you can’t track who has logged in to the server.

Note: In Macintosh Manager 2.0, the workgroup data volume is separate from the user’s document storage volume. The workgroup data volume contains the global shared folder, the shared workgroup folder, and the Managed Preferences folder. User documents, on the other hand, are stored in the home directory volume, as defined in Mac OS X Server Users & Groups.

Always try auto log-in with user’s name and password first

If you select this option, the computer attempts to log in to the workgroup volume with the user’s Macintosh Manager name and password (imported from your Mac OS X Server database).

Group Message

Enter the message that you want to appear whenever a user logs in to the workgroup.

Startup and Log-In

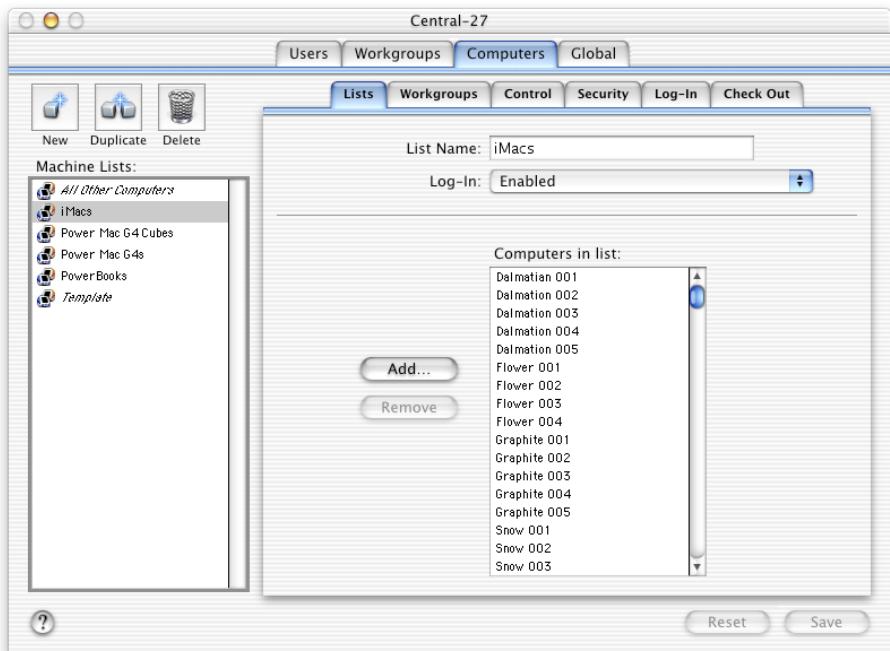
- Select “Open items in the Startup Items folder” to open items in the user’s designated Startup Items folder automatically when the user logs in. The designated folder for Mac OS 9 and later computers is the /Library/Startup Items directory on the Macintosh Management server. The designated folder for pre-Mac OS 9 computers is the Startup Items folder in the System Folder on the client’s hard disk.
- Select “Check for email when members log in” to check for email at login if a user has a POP email account. If the user doesn’t already have an email address, you may need to provide mail server settings in the Control pane of the Computers pane so that Macintosh Manager can generate an address.
- Select “Copy preferences when workgroup members log in” to copy the preferences you set in the Security pane of the Global pane at login (for pre-Mac OS 9 client computers only). You don’t need this setting for client computers with Mac OS 9 or later installed because preferences reside on the server and do not need to be copied.

Ejecting CD-ROM discs

Select “Require an administrator password to eject CD-ROM discs” to require that a workgroup administrator or Macintosh Manager administrator name and password be entered to eject CD ROM discs (this doesn’t apply to Finder workgroups).

Lists Settings for Computers

The settings you make in the Lists pane apply to all computers in the currently selected computer list. Computer lists let you further refine who can get access to computers and workgroups. For example, a workgroup made up of staff members can be required to use a specific set of computers. No one who logs in to any other computers on the network—including the staff members themselves—will be able to get access to the staff workgroup. This allows the administrator greater flexibility in controlling access to software and hardware.



List Name

The list name can contain most keyboard characters (including the period, underscore, dash, and space) except a colon (:), and can contain no more than 31 characters.

Log-In

The Log-In pop-up menu has four options:

- “Enabled” lets users log in. You usually have this selected unless you need to do maintenance tasks on your computers, such as installing software or running hard disk maintenance software.
- “Disabled - Ask User” lets the user choose to shut down the computer, go to the Finder (an administrator password is required), or pick a new Macintosh Manager server.
- “Disabled - Go to Finder” automatically logs the user in to the Finder.

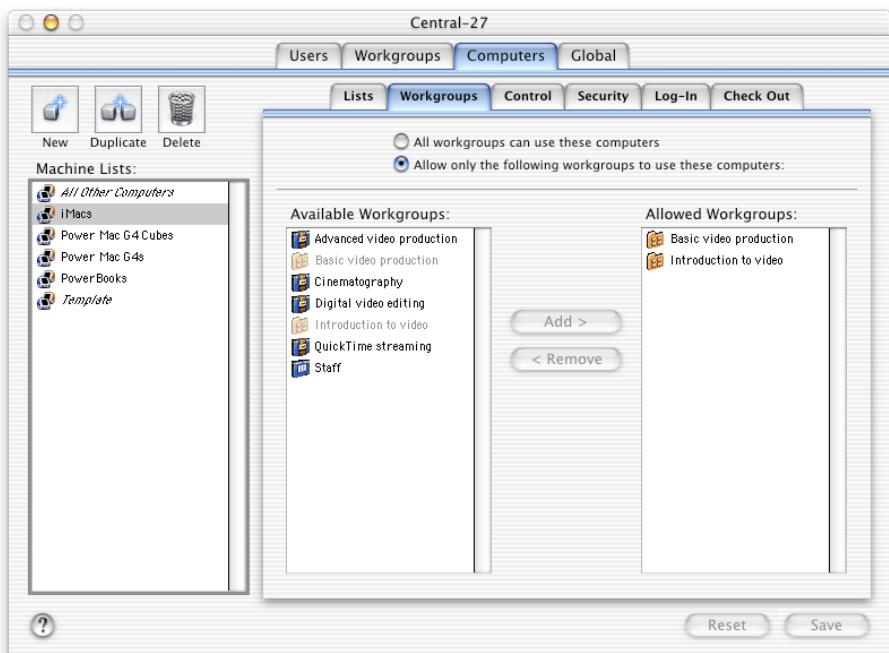
- “Disabled - Pick different server” prompts the user to select another Macintosh Management server.

Computers in list

This field shows all the computers in the selected list. To add a computer to the list, click Add. To remove a computer, select it and click Remove.

Workgroups Settings for Computers

You can use the Workgroups pane of the Computers pane to restrict the use of computers on a list to specific workgroups. For example, in a school you may want to allow only users in the Teachers workgroup to log in to computers located in the teachers' lounge.



All workgroups can use these computers

Select this option to allow users in all workgroups to use any of the computers in the selected computer list or lists.

Allow only the following workgroups to use these computers

Select this option to specify which workgroups can use computers in the selected list or lists.

Available Workgroups

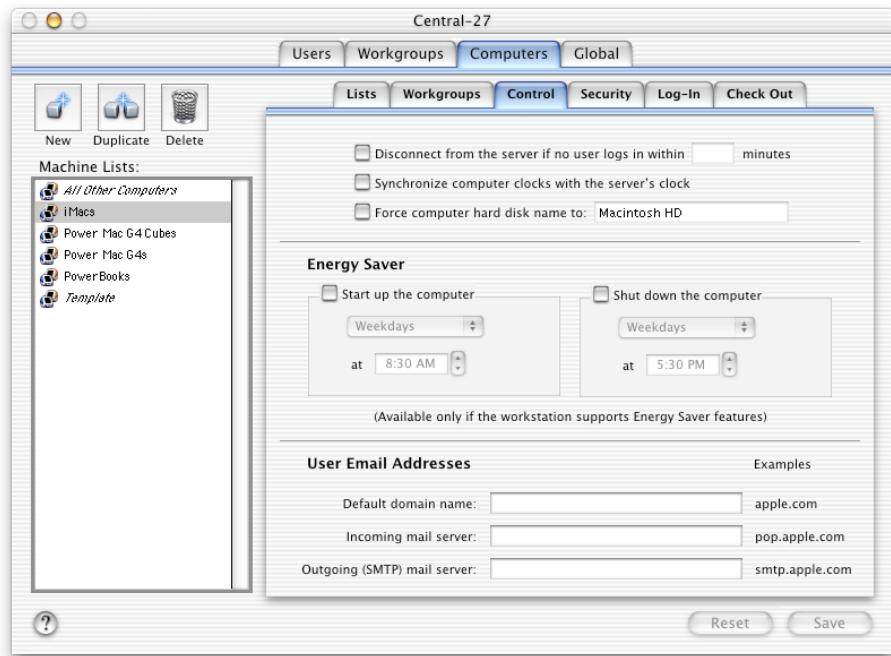
This list shows all your Macintosh Manager workgroups. The list is available only if you select “Allow only the following workgroups to use these computers” above. To give a workgroup access to a computer in the selected computer list, select the workgroup and click Add.

Allowed Workgroups

This list shows the workgroups to which you’ve given access to computers in the selected computers list.

Control Settings for Computers

The settings you make in the Control pane of the Computers pane apply to all computers in the currently selected computer list.



Disconnect from the server if no user logs in within _ minutes

If you select this option, the computer stops querying the server after the number of minutes you enter. The computer still displays the login screen and has a green X over the server icon in the menu bar. The computer no longer checks the server for updates or other traffic until a user logs in again. Using this setting keeps network traffic to a minimum, but also keeps automatic updates from occurring until a user logs in and out again.

Synchronize computer clocks with the server's clock

Selecting this option synchronizes computer clocks with the clock on the server, if your network does not have access to a Network Time Protocol server.

Force computer hard disk name to

Select this option and enter a name to have Macintosh Manager change the name of the client hard disk to the name you specify. This option is meant primarily for use with NetBoot clients, for whom the startup volume is named “NetBoot HD” by default. By forcing the name to, for example, “Macintosh HD,” you can ensure that the path names for all applications used on these clients will be the same as those for non–NetBoot computers. This is optional for non–NetBoot computer environments.

Energy Saver

Energy Saver settings let you set automatic startup and shutdown times for client computers that have the energy-saving feature. To find out if you can use this setting with a computer, check to see if the Energy Saver control panel (version 2.0 or later) is in the computer’s Control Panels folder. Some computers sleep instead of shutting down based on the settings you select.

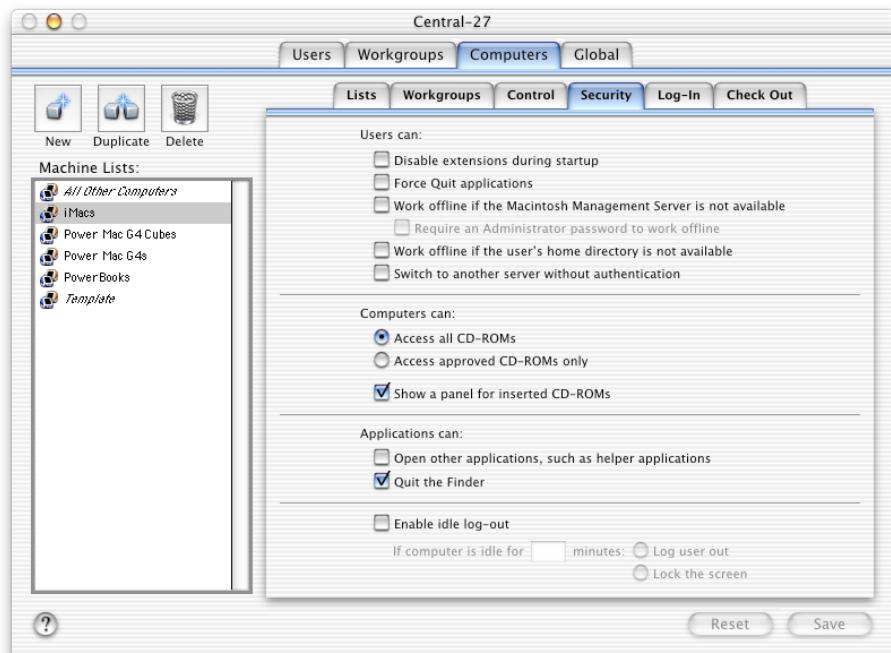
User Email Addresses

Macintosh Manager can create an email address for users who don’t have one, by using the user’s alias and the domain name you specify in the “Default domain name” field. You also need to enter the POP (incoming mail) and SMTP (outgoing mail) server addresses. Any imported email settings will override Macintosh Manager email settings when users connect to the Macintosh Manager network.

To have the computer check for messages when the user logs in, select “Check for email when members log in” in the Options pane of the Workgroups pane.

Security Settings for Computers

The settings you make in the Security pane of the Computers pane apply to all computers in the currently selected computer list.



Users can

- Select “Disable extensions during startup” to let users disable extensions by pressing the Shift key during startup. Pressing the Shift key never disables Macintosh Manager extensions, but it disables other extensions.
- Select “Force Quit applications” to let users force quit an application by pressing Command-Option-Esc. This may be a security risk.
- Select “Work offline if the Macintosh Management Server is not available” to let users use the computer if the server volume is not available.
- Select “Work offline if the user’s home directory is not available” to let users work offline if the volume that stores their home directory is not available.
- Select “Switch to another server without authentication” to let client computers switch to another Macintosh Management server without an administrative password. If enabled, this option can decrease security. Use it with care if you have servers with older versions of the Macintosh Management server software. Switching a client computer to an older server may cause it to install older client software.

Computers can

- Select “Access all CD-ROMs” to let users access all CD-ROM and DVD-ROM discs.
- Select “Access approved CD-ROMs only” to limit access to a list of approved discs. If you select this setting, you must set up a list of approved discs in the CD-ROMs pane of the Global pane.
- Select “Show a panel for inserted CD-ROMs” to display a panel when a CD-ROM is inserted (for the Panels environment).

Applications can

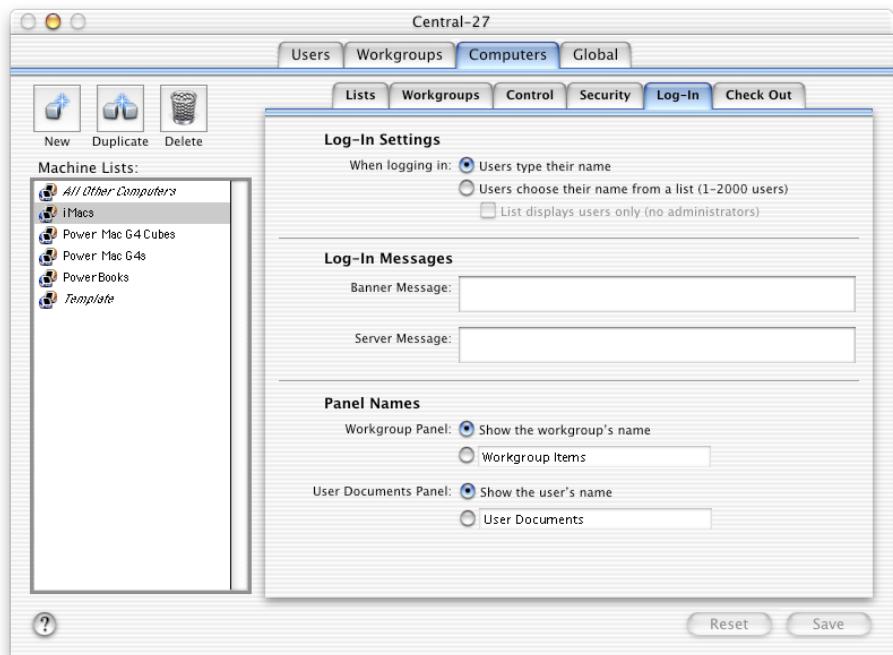
- Select “Open other applications, such as helper applications” to let applications open helper applications as needed. Without this setting enabled, applications can’t open other applications that provide certain features to users. For example, Web browsers can’t open helper applications, such as PictureViewer. Enabling this setting may create a security weakness.
- Select “Quit the Finder” to let applications, such as Installers, quit the Finder on Mac OS 9 computers. Enabling this option may let some applications bypass security. If you don’t select this option, applications that need to be able to quit the Finder may not work properly.

Enable idle log-out

Select this option and enter a number of minutes to set how much time can pass with the computer left inactive before users are logged out of their workgroup or the screen is locked. If you select “Log user out,” the user is given the opportunity to save any unsaved documents, then is returned to the login screen. The user cannot exit the Save dialog and continue working. If you select “Lock the screen” the screen goes blank and a dialog appears to let the user choose between logging out or entering a password to continue working.

Log-In Settings for Computers

The settings you make in the Log-In pane of the Computers pane apply to all computers in the currently selected computer list.



Log-In Settings

You can choose one of two options for how users log in to a computer:

- Select “Users type their name” to require users to manually enter their name in the login dialog. This is usually faster and offers more security than selecting names from a list, but it requires users to know their user names.
- Select “Users choose their name from a list (1–2000 users)” to let users scroll through a list to find their name. This is usually slower because it can take awhile for the list to appear if you have more than 100 users. You cannot use this option if you have 2000 or more Macintosh Manager user accounts.

Log-In Messages

You can create two types of login messages (with up to 127 characters):

- “Banner Message” appears in the login dialog for the selected computer list.
- “Server Message” appears after users log in to a computer in the selected list.

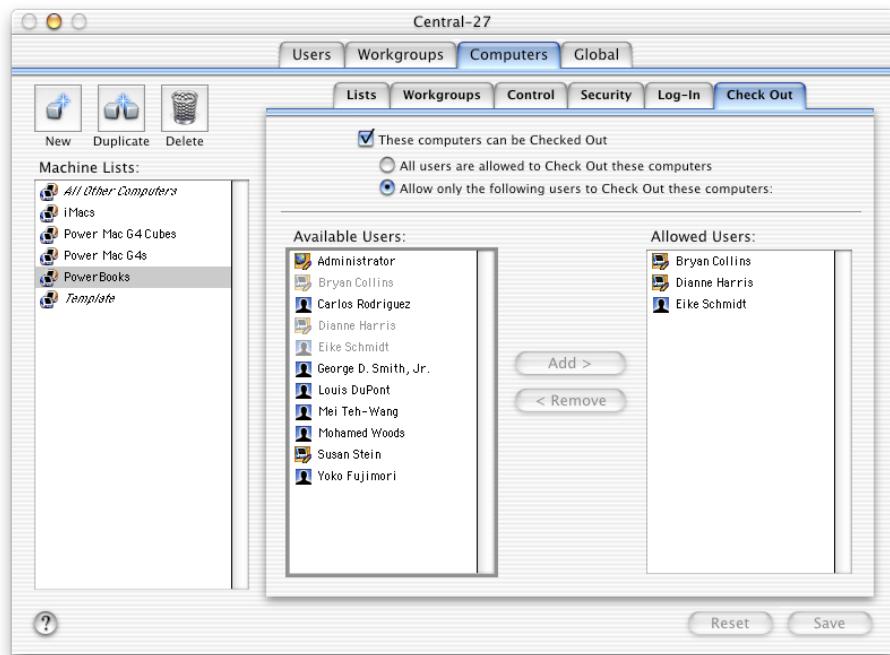
Panel Names

You can customize the names of the workgroup and user documents panels in the Panels environment.

- Select “Show the workgroup’s name” to display each workgroup’s name on its workgroup documents panel. Or, click the button below and type another name in the field.
- Select “Show the user’s name” to display each user’s name on his or her documents panel. Or, click the button below and type another name in the field.

Check Out Settings for Computers

You can allow users to check out computers using the Check Out pane of the Computers pane. For example, a user could check out and take home a portable computer to continue working on a project after school. The Macintosh Manager security features will still remain in force on the computer even while it’s checked out.



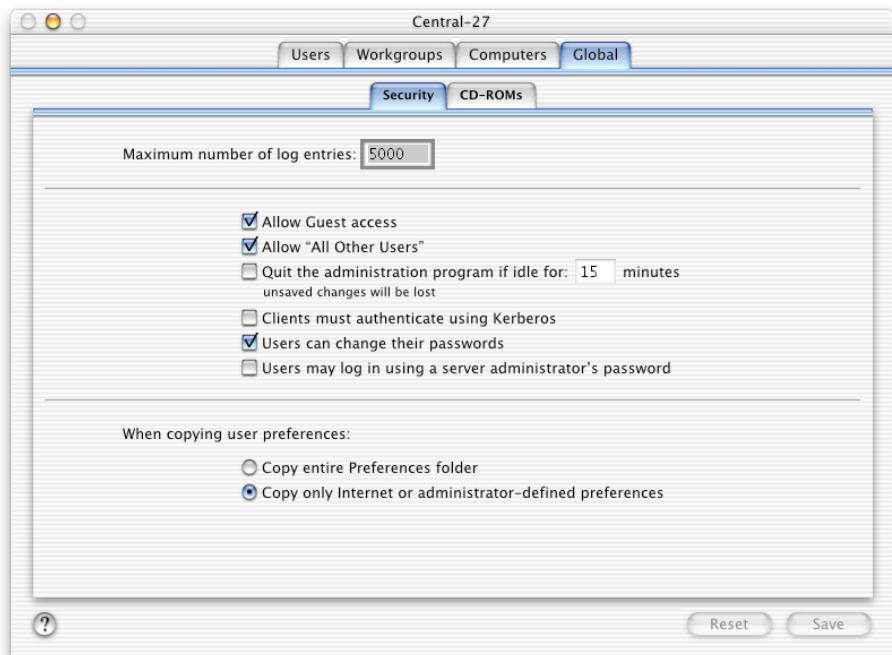
These computers can be Checked Out

Select this option to enable users to check out computers in this computer list.

- Select “All users are allowed to Check Out these computers” to allow any user to check out any computer in this list.
- Select “Allow only the following users to Check Out these computers” to restrict check out to the users you select.

Global Security Settings

The options in the Security pane of the Global pane let you ensure the integrity of your Macintosh Manager network and protect your users' documents from tampering.



Maximum number of log entries

Enter the maximum number of log entries that should be included in the server's activity log. You can view the log using the Report menu.

Allow Guest access

Select this option to let guest users log in (if the Guest user has been added to a workgroup).

Allow All Other Users

Select this option to let any user with a Users & Groups name and password log in to a client computer, even if the user hasn't been imported into Macintosh Manager.

Quit the administration program if idle for _ minutes

Select this option and enter the number of minutes after which the Macintosh Manager administration program quits if it hasn't shown any activity.

Clients must authenticate using Kerberos

Select this option if you want client login information to be verified using the Kerberos network authentication protocol.

Users can change their passwords

Select this option to let all users change their passwords. If you choose to disable the privilege, the option to change a password is unavailable in the user's login dialog.

Users may log in using a server administrator's password

Select this option to allow the system administrator to log in to any user's account using that user's name and the administrator password.

When copying user preferences

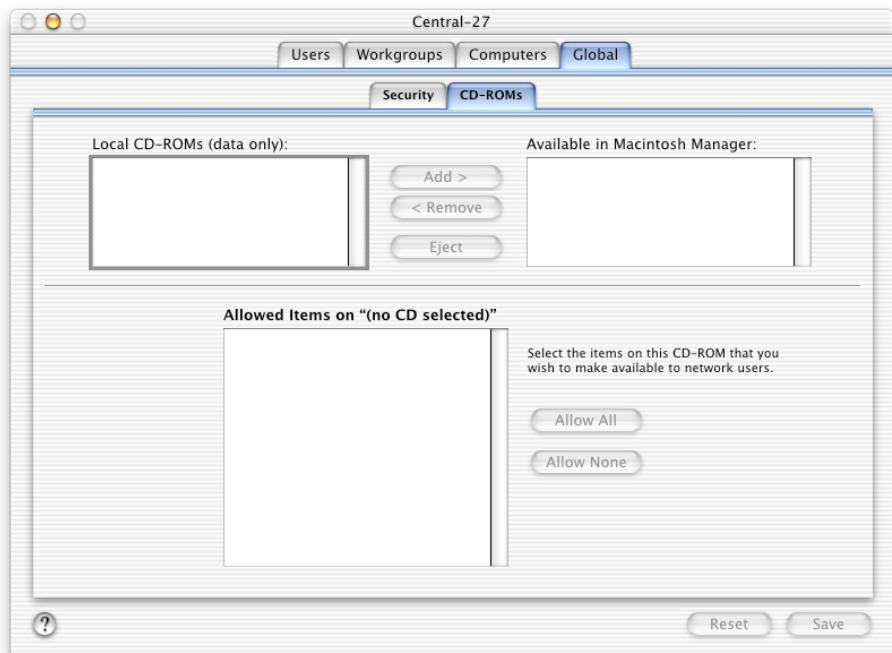
The next two settings control how user preferences are copied for pre-Mac OS 9 client computers. Users can change their preferences (such as the desktop picture) while logged in to a pre-Mac OS 9 client computer. However, when the user logs out, preferences are saved only if you allow them to be saved.

- “Copy entire Preferences folder” forces Macintosh Manager to copy all items in the Preferences folder regardless of what the item is or how large it is. Be aware that copying unnecessary or large items can increase login and logout times.
- “Copy only Internet or administrator-defined preferences” sets Macintosh Manager to copy these files and folders whenever a user logs in:
 - StuffIt Expander Preferences
 - RealAudio™ Player Preferences
 - Internet Preferences
 - NCSA Telnet Preferences
 - Fetch Prefs
 - NewsWatcher Prefs
 - JPEGView Preferences
 - Netscape f
 - Explorer

For Netscape and Explorer, the folders are copied, but the cache folders inside them are deleted.

Global CD-ROMs Settings

Using the CD-ROMs pane of the Global pane, you can allow access to all CD-ROM and DVD-ROM discs, or you can limit access to a list of discs. When you add a disc to the list of available discs, you can view its contents. You can allow users to access all items on the disc, or just items that you choose.



To allow use of audio CDs, use the Privileges pane of the Workgroups pane.

Macintosh Manager Strategies and Tips

This section includes hints and advice on using Macintosh Manager efficiently.

Providing Quick Access to Unimported Users

The quickest and most convenient way to grant authenticated access and set up customized environments for users is to use the All Other Users account in the Imported Users list. If you enable login for the All Other Users account, users with accounts in the Mac OS X Server Users & Groups database can log in to client computers even if they haven't been imported into Macintosh Manager. They'll have the access privileges and environment you set up for the All Other Users account in Macintosh Manager and they can access their home directories, preferences, and documents. (The All Other Users feature is different from Guest access since guests don't get password authentication and can't store files or preferences.)

For example, in a university with a central user database, a computer lab's Macintosh Management service can be set up with only the All Other Users account. Any user on campus with a Mac OS X Server account can walk into the lab, log in, and get access to their home directory, preferences, and documents. They don't have to be individually imported into Macintosh Manager first.

Note: The All Other Users account cannot be used to check out computers or to work at a client computer offline. Disk quotas are not enforced for users who are logged in using the All Other Users account.

Setting Up All Other Users

To set up the All Other Users account:

- 1 If the All Other Users account doesn't appear in the Imported Users list in Macintosh Manager, click the Security tab of the Global pane, and then click Allow "All Other Users."
- 2 Click the Users tab and select All Other Users in the Imported Users list.
- 3 Make whatever changes you want in the Basic and Advanced panes of the Users pane.
- 4 Click the Workgroups tab and add the All Other Users account to a workgroup.
- 5 Change the settings for the workgroup to what you want them to be for the All Other Users account.
- 6 Make sure computers have been made available to the workgroup in the Computers pane.

How All Other Users Appears at Login

If you have set up your client computers to require users to type their names and passwords when they log in, users can simply type their Mac OS X Server name and password in the Macintosh Manager login dialog. If you let users choose their name from a list when logging in, All Other Users appears at the top of the list, directly below Guest. When users choose the All Other Users account, a login dialog appears, where they can type their Mac OS X Server name and password.

Setting Up Macintosh Manager on Large or Growing Networks

If you have a large network with many users, you may need more than one server volume. Or you may anticipate that your network will eventually require another server or partition, and you want to set it up in a way that will make the transition easy. The solution is to set up the network with additional servers to store shared group files, home directories, clip art folders, department or class Web sites, shared CDs, and special network applications. This way, once users log in to Macintosh Manager, they can access content in other share points, including ones that reside on other volumes. You select where shared group files are stored in the Options pane of the Workgroups pane.

A major benefit of setting up multiple share points is that it lets you keep related files in manageable groups. And, if you need to add a hard disk partition or another server, you can easily move the share points to those new volumes.

Creating Workgroups to Meet Your Network's Needs

Most settings you make in Macintosh Manager are for workgroups of users, rather than for individual users. In order to designate a setting for a user, you need to put the user into a workgroup.

When setting up workgroups, think in terms of common projects and the needs of those projects. For example, ask yourself these questions:

- Do you want some of your users (such as guest users) to have a restricted desktop environment, including limited access to certain menu items, local folders and applications, and so on?

If so, create a workgroup for those users and assign that desktop environment to that workgroup. See “Choosing Desktop Environments for Your Workgroups” on page 230 for more information.

- Do you want some users to have easy access to certain applications and files? If yes, create a workgroup that gives the users that access.
- Do some users need to work on documents collaboratively, and thus need access to a shared folder?

If so, make sure there is a workgroup made up of just those users, and set up a shared workgroup folder.

- Do you want some of your users to check work into a folder that only administrators (for example, teachers or supervisors) can open?
If so, create a workgroup for just those users, and set up a hand-in folder for that workgroup.
- Do you want some of your users to have special access to a certain printer?
If so, make sure there is a workgroup made up of just those users, and give them access to that printer.
- Do you want to restrict usage of certain computers to a specific group of users?
If so, create a workgroup with just those users, use the Computers pane to create a list that includes those computers, then assign that workgroup to that computer list.

Remember, you can assign a user to more than one workgroup.

Choosing Desktop Environments for Your Workgroups

The workgroup desktop environment determines the interface that users in a workgroup see, and the type of access workgroup members have to network resources.

In the Members pane of the Workgroups pane, you choose from the following types of environments.

Environment	Description	When to use it
Finder	<ul style="list-style-type: none">■ Looks and acts like the standard Mac OS desktop.■ Users have unrestricted access to all applications on their local hard disk.■ Users' home directories are mounted at login and users are restricted from using certain control panels.	When you want your users to have maximum flexibility, and the administrator's control is not a top priority

Environment	Description	When to use it
Restricted Finder	<ul style="list-style-type: none"> ■ Looks like the standard Mac OS desktop, but restricts what users can do. ■ Users can browse their local hard disk, but the administrator determines what users can open on their computer. 	When you want to choose what can be opened on client computers, while providing users access to the standard Mac OS desktop
Panels	<ul style="list-style-type: none"> ■ Simple interface with large icons that make using a computer easy for novice users. Users can only see and access items assigned to their workgroup(s). ■ If you allow access to server volumes or removable media, each volume or media appears as a panel when it is mounted. ■ You can specify panel names (in the Log-In pane of the Computers pane). 	When you want to provide users with the most simple environment, and/or when you want the administrator to have maximum control over what users can do with their computer

Maximizing Security

There are a number of ways to maximize security when using Macintosh Manager. See Macintosh Manager Help for details on how to

- prevent access by people who are not registered users
- prevent changes to the startup environment, system settings, and other administrative options
- prevent applications from bypassing security
- prevent applications from opening other applications
- limit access to CDs
- restrict use of applications on removable media

To access the onscreen help, choose Macintosh Manager Help from the Help menu or click the question mark in the bottom-left corner of any of the panes in the Macintosh Manager window.

Inside Macintosh Manager

This section contains “behind the scenes” information about how Macintosh Manager works. You may find this information especially useful when you troubleshoot problems.

How Macintosh Manager Starts Up

When a client computer starts up, and a user logs in, the following happens:

- A login dialog appears. Users either type a name or choose a name from a list, depending on how you’ve set up Macintosh Manager.
- Macintosh Manager validates the user name and password using the Mac OS X Server directory. Then, Macintosh Manager checks its own databases to see if the user has an account.
- If the user belongs to more than one workgroup, the user chooses one from a list of his or her workgroups.
- Macintosh Manager locates and opens the user, workgroup, and computer databases.
- The workgroup environment and other settings are enabled.
- The user sees server and workgroup login messages, if there are any.
- The user sees an alias to his or her documents folder on the desktop (unless the user is in the Panels environment).

How Macintosh Manager Works With Preferences

This section describes how user-specific preferences (such as Web browser “favorites” and desktop backgrounds) are stored in a Macintosh Manager environment, and how an administrator can control preferences using a Managed Preferences folder. There are some differences in how preferences are handled on Mac OS 9 and pre–Mac OS 9 computers. These differences are described where appropriate.

Where Preferences Are Stored

By default, preferences are stored and accessed in this way:

- *When a client is not logged in:* Most of his or her individual preferences are stored on the server, for both Mac OS 9 and pre–Mac OS 9 client computers.
- *When a client user logs in to Macintosh Manager:* The individual preferences for that user are located by Macintosh Manager and put in effect for as long as the user is logged in. Where the preferences are stored while the user is logged in depends on whether the client computer has Mac OS 9 or an earlier version of the Mac OS:
 - *For pre–Mac OS 9 clients:* Preferences are stored in the Preferences folder in the System Folder on the client computer’s hard disk.
 - *For Mac OS 9 clients:* Preferences are stored in the /Library/Preferences folder in the user’s home directory.

In some cases, preferences for Mac OS 9 users may be stored in the Preferences folder in the Users folder on the client hard disk, but not in the Preferences folder in the System Folder.

Using Managed Preferences

You can also use “managed preferences” to customize how preferences are handled to meet your specific needs and goals. For example, you can make sure that users always start out with a set of preferences you’ve defined, or that some user-set preferences are never overridden.

You can group managed preferences into three categories: initial preferences, forced preferences, and preserved preferences. Whether you can use these categories depends on the version of the Mac OS on the client computer:

	Mac OS 9 clients	Pre-Mac OS 9 clients
Initial preferences	Yes	Yes
Forced preferences	Yes	Yes
Preserved preferences	No	Yes

The Managed Preferences folder (and the Initial Preferences, Forced Preferences, and Preserved Preferences folders inside it) is created the first time any member of a workgroup logs in.

To use managed preferences:

- 1 Set up a workgroup data volume in the Volumes pane of the Workgroups pane.
- 2 From a client computer, log in to the workgroup data volume.
- 3 Create any preferences you want to place in the Initial or Forced Preferences folders.
- 4 Copy the preferences you created to the Initial or Forced Preferences folders on the workgroup data volume.
- 5 If you want to create any preserved preferences for pre–Mac OS 9 client computers, place files and/or folders with the names of those preferences in the Preserved Preferences folder.

If the actual preference is in the form of a file, then the item of the same name you place in the Preserved Preferences folder must be a file. Likewise, if the real preference is a folder, then it must be a folder.

- 6 Repeat steps 1 through 5 for each workgroup data volume.

For more information on using each kind of managed preference, see the following sections.

Initial Preferences

The Initial Preferences folder lets you give each user a specific set of preferences once during login. If the user already has a preference in the Initial Preferences folder, Macintosh Manager doesn't replace the user's preference. This process is repeated each time a user logs in, so you can place additional preference files in the Initial Preferences folder later if you install additional software. When a user opens the new software for the first time, a copy of the preference files for the new software will be moved to his or her Preferences folder.

A few preferences are created the first time a user logs in, regardless of whether you're using an Initial Preferences folder. If you place these items in the Initial Preferences folder, they won't be copied to the user's folder:

- Apple Menu Options Prefs
- AppSwitcher Preferences
- Internet Preferences
- Keyboard Preferences
- Keychains
- Location Manager Prefs
- Mac OS Preferences
- TSM Preferences
- User Preferences

Example: When to use the Initial Preferences folder

Let's say you want to provide all your users with a set of preconfigured bookmarks and preferences for Internet Explorer, but only for the first time they log in. To do so, you'd follow these steps:

- 1 Set up the bookmarks and preferences you want on your administration computer.
- 2 Open the Preferences folder in the System Folder on your administration computer and locate the Explorer folder. Copy the entire Explorer folder to the Initial Preferences folder on the Macintosh Manager server.

Here's what happens when a client logs in:

- *When a Mac OS 9 client logs in:* Macintosh Manager looks for a folder named Explorer in the /Library/Preferences folder in the user's home directory. If Macintosh Manager doesn't find an Explorer folder already in the user's folder, it copies the new Explorer folder (and its contents) from the Initial Preferences folder to the user's folder.

If there's already an Explorer folder in the user's folder, Macintosh Manager updates the existing folder, replaces older files with newer files that have the same names, and adds any files that you've put in the Forced Preferences folder since the last time the client logged in. If there are files or folders in the user's Preferences folder with unique names that don't match files in the Forced Preferences folder, Macintosh Manager does nothing to them. To prevent files accumulating and consuming disk space, check the user's Preferences folder as often as you think necessary.

- *When a pre-Mac OS 9 client logs in:* Macintosh Manager looks for a folder named Explorer in two places: the user's Preferences folder in the user's home directory, and the Preferences folder in the System Folder on the client computer. If Macintosh Manager doesn't find the folder in the user's Preferences folder, it places a copy of the Explorer folder in the user's Preferences folder, as well as in the Preferences folder on the client computer, replacing any copy that exists there. If the folder already exists in the user's Preferences folder, no copying takes place.

Note: For pre-Mac OS 9 computers, if Macintosh Manager can't find an Explorer folder in just one of the two locations it checks, it copies the Explorer folder just to that location. This can result in an inconsistent user experience if the user moves from one client computer to another.

Forced Preferences

The Forced Preferences folder lets you force users to start with a set preferences you specify every time a user logs in. If a user changes his or her preferences, those preferences will be replaced with the preferences in the Forced Preferences folder the next time the user logs in.

Example: When to use the **Forced Preferences** folder

Let's say you want to provide all your users with a set of preconfigured bookmarks and preferences for Internet Explorer every time they log in. To do so, you'd follow these steps:

- 1 Set up the bookmarks and preferences you want on your administration computer.
- 2 Open the Preferences folder in the System Folder on your administration computer and locate the Explorer folder. Copy the entire Explorer folder to the Forced Preferences folder on the Macintosh Manager server.

Here's what happens when a client logs in:

- *When a Mac OS 9 client logs in:* Macintosh Manager looks for a folder named Explorer in the /Library/Preferences folder in the user's home directory. If Macintosh Manager doesn't find an Explorer folder already in the user's folder, it copies the new Explorer folder (and its contents) from the Forced Preferences folder to the user's folder. If there's already an Explorer folder in the user's folder, Macintosh Manager deletes the existing folder and replaces it with the Explorer folder in the Forced Preferences folder.

- *When a pre-Mac OS 9 client logs in:* Macintosh Manager copies the Explorer folder from the Forced Preferences folder to the Preferences folder in the System Folder on the client computer, regardless of whether other copies already exist. No files or folders are copied to the user's Preferences folder in the home directory.

Preserved Preferences

The Preserved Preferences folder only works with pre-Mac OS 9 client computers. The files and folders that you put in the Preserved Preferences folder are never actually copied.

Macintosh Manager scans the files and folders in the Preserved Preferences folder, and builds a list containing the names of all the items inside. Macintosh Manager then uses this list to determine which preferences need to be copied between the server and the client computer during login and logout. Because the Preserved Preferences folder lets you limit which preferences are copied, using it can help you decrease login and logout time.

Some preferences are always copied, whether or not they exist in the Preserved Preferences folder, and some are never copied, even if they exist in the Preserved Preferences folder:

Preferences that are always copied	Preferences that are never copied
Control Strip Preferences	AppleTalk Preferences
Date & Time Preferences	Client Prefs
Finder Preferences	ColorSync Profiles
Mac OS Preferences	Desktop Picture Prefs
Panels Preferences	Energy Saver Preferences
	Extensions Manager Preferences
	Multi-User Items
	Multi-User Prefs
	Open Transport Preferences
	Remote Access
	TCP/IP Preferences
	Users & Groups Data File
	Users & Groups Data File Backup

- *When a user logs in on a pre-Mac OS 9 client computer:* Macintosh Manager scans the Preserved Preferences folder and builds a list containing the names of the files and folders inside. Macintosh Manager then adds the names of the items in the “always copied” list to create a combined list. Macintosh Manager then copies all the files and folders included in the combined list from the user’s Preferences folder on the server to the client computer’s Preferences folder. Any existing files and folders in the client’s Preferences folder that have the same name as those in the combined list are deleted. If an item in the list does not exist in either the user’s Preferences folder on the server or the Preferences folder on the client computer, the item is skipped.
- *When the user logs out:* Macintosh Manager uses the same process to determine which preferences are copied from the client computer’s Preferences folder back to the user’s Preferences folder on the server. All items matching those on the combined list are deleted from the Preferences folder on the client computer.

Note: A user who logs in using the System Access workgroup may not be able to use some applications, because the preferences for the applications were deleted from the Preferences folder after the last user logged out.

How Macintosh Manager Ensures Security

Macintosh Manager is designed so that users at client computers can’t disable system extensions by holding down the Shift key as the computer starts up. Users cannot turn Macintosh Manager off in the Extensions Manager control panel, nor can they move the Macintosh Manager extensions from the Extensions folder in the System Folder.

Macintosh Manager has a number of other safeguards to ensure security. The following safeguards work in all of the desktop environments. Many of these are enabled by default, and some can be deactivated by the Macintosh Manager administrator:

- All of the environments restrict users from altering certain system settings. These include network settings (AppleTalk and TCP/IP control panels), Energy Saver settings, and Multiple User settings.
- Users are denied access to other users’ home directories, regardless of workgroup.
- Users cannot rename Macintosh Manager files, or change the file type or creator.
- When a user shuts down or restarts the computer, user changes are saved.
- Users can’t force quit an application to get around Macintosh Manager security. (You must enable this option in the Security pane of the Computers pane.)
- Users can’t eject removable media or unmount server volumes without an administrator password. (You must enable these options in the Options pane of the Workgroups pane or in the Security pane of the Computers pane.)

How Client Computers Are Updated From the Server

A copy of the Multi-User Items folder, which contains information about your Macintosh Manager settings, is stored automatically in the System Folder of each client computer (for more information about the Multi-User Items folder, see “About the Macintosh Manager Share Point” on page 239). This folder lets your users work offline and optimizes performance because Macintosh Manager can look up information more quickly on the client computer. The Multi-User Items folder contains information about the location of the Macintosh Management server, so users usually don’t have to choose a server before they can log in. A Multi-User Items Cache folder is also created inside the Multi-User Items folder, inside the Preferences folder. This cache folder contains items that speed up login.

If the client’s Multi-User Items folder is deleted, the client downloads a new, clean copy from the server. The client’s Multi-User Items folder is also updated when you make changes in Macintosh Manager. When a client computer is connected to the server, but no users are logged in, Macintosh Manager checks periodically to see if any items need to be updated. Macintosh Manager does not check for changed information if a user is logged in to a computer—updating doesn’t happen until the user logs out. If a computer is disconnected from the server automatically because it was idle for a period of time, no update checks are made until a user logs in and out of the workstation.

How Macintosh Manager Keeps Track of Users, Workgroups, and Computer Lists

Information about users, workgroups, and computers is stored in database files located in the Users, Groups, and Computers folders. (These folders are located in the Multi-User Items folder in the Macintosh Manager share point, described in the next section.) Each folder contains two database files. One file contains an index of each record in the database (such as the name of a workgroup) and the other file contains the specific information for each record (such as workgroup members, privileges, and environment).

Although the users, groups, and computers databases are not part of a larger relational database, each refers to information stored in the other databases. For example, the users database contains a list of workgroups that a user belongs to. To maintain consistency between databases, Macintosh Manager checks references from one database to another and updates the databases as needed. You do not need to do anything to the databases for them to function properly. If you attempt to modify the databases directly, you will introduce inconsistencies and may lose the information stored in them. If this occurs, you’ll need to re-create user, workgroup, and computer information by using the Macintosh Manager administration program, or by restoring information from a backup copy.

About the Macintosh Manager Share Point

When Macintosh Management server software is installed, a share point named Macintosh Manager is created on the server. It's set up with the correct permissions so Macintosh Manager can access the share point. The Macintosh Manager share point exists primarily to service the database. Users can't see the contents of the share point and do not interact with it.

You can move the Macintosh Manager share point to another volume as long as the name of the share point is the same, the folder remains a share point, and the access privileges are the same.

The Multi-User Items folder

The Multi-User Items folder is located in the Macintosh Manager share point. It contains information about options you set using Macintosh Manager, such as the location of the Macintosh Management server, aliases to workgroup items, cache information, and the databases for users, groups, and computer lists. The Multi-User Items folder contains the following:

- *Activity Log*: This file contains log entries. It is used to generate reports such as the printer usage and activity reports.
- *CD-ROM Prefs*: This file contains a list of CDs users are allowed to use, along with settings for specific items on each CD.
- *Computers*: This folder contains database files that store Macintosh Manager settings for each computer list you set up.
- *Groups*: This folder contains a folder for each workgroup and database files that store Macintosh Manager settings for each workgroup. A compressed version of the workgroup's items are stored on the server. (Aliases to the items are stored on the client computer.)
- *Multi-User Items file*: This file contains an archive of the files currently inside the Multi-User Items folder. Do not open or modify the file. If it is deleted, it is re-created the next time you use Macintosh Manager.
- *Printers*: This folder contains files that represent the desktop printers you set up in Macintosh Manager. A file is created for each desktop printer used by a workgroup. When a user logs in to a workgroup that uses a desktop printer, the printer file is copied to the desktop of the client computer.

You should use Macintosh Manager to modify printer information; don't open or remove items in the Printers folder. If you delete a printer file from this folder, workgroup members who want to use that printer see a message that the printer can't be found.

- *Users*: This folder contains database files that store Macintosh Manager settings for each user account and a folder for each user that has logged in to the server at least once.

Using Macintosh Manager and NetBoot Services Together

Although you do not need to use NetBoot with Macintosh Manager, doing so makes it even easier to manage each computer's system setup in labs and classrooms.

To use NetBoot with Macintosh Manager, use the NetBoot Desktop Admin utility to change the Multiple Users control panel options so that NetBoot client computers retrieve account information from Macintosh Manager when they start up (see "Using NetBoot Desktop Admin" on page 255).

Example: An Elementary School Equips a New Computer Lab

The school has these technology objectives:

- Support educational goals in various areas of instruction, such as reading and math.
- Ensure that each computer has the same software.
- Promote desktop security by protecting the computer and network resources from student tampering.
- Set up a network that's easy to maintain.
- Provide centralized document storage.

These networking strategies will support the technology objectives:

- Use one server that contains the Mac OS image that NetBoot client computers use to start up from, and has the Macintosh Management server software installed. The server will also store users' documents and applications.
- Use Macintosh Manager to set options that promote desktop security.
- Set up workgroup administrator accounts for teachers, then show them how to use Macintosh Manager to manage user accounts and workgroups.
- Set up the client computers to start up from the Mac OS image on the server.

Because the client computers use system software supplied by the NetBoot server, you can ensure that each computer has the same version of software and access to the same applications. Regardless of what users change during a session, the computers return to the same system configuration after users log out.

You can ensure desktop security by using Macintosh Manager to control which network resources students can access. You can protect the System Folder and Applications folder, and you can set options that promote security when using applications.

The network is easy to maintain because the user applications need to be installed only on a disk image stored on the server. Once the network is set up, there is very little daily management. The teacher can manage user accounts and workgroups from any computer connected to the server. Teachers can distribute and collect assignments over the network. A teacher can also make available network resources, applications, and CDs that promote teaching objectives for the class.

Solving Problems With Macintosh Manager

This section covers some problems you may encounter while using Macintosh Manager. When solving complex problems, it might also be helpful to refer to “Inside Macintosh Manager” on page 232.

Problems Logging In to Macintosh Manager

If you've forgotten an administrator password:

Contact your Mac OS X Server system administrator or change the administrator password using the Server Admin application.

If a user can't open a file (such as a media file) from a Web page:

Check whether the user's workgroup settings allow applications to open other applications. (See the Security pane of the Computers pane.) If you want users to be able to open applications from Web pages, select “Open applications, such as helper applications” in the Applications Can box.

If the client computer can't find or connect to the server:

- Make sure the server is running. It may take a few minutes for the server to appear if you have just started it up.
- If your network has AppleTalk zones, users on pre-Mac OS 9 computers may need to select the zone in which your server resides. On Mac OS 9 computers, use the Network Browser to make sure you are connected to the server. For best performance, it is recommended that you set client computers to connect to the server over TCP/IP, not AppleTalk.
- Check that the client computer is not low on memory and is still connected to the network.
- If many computers are starting up at once, the network load may be too high. Try starting up fewer computers at once.

If you can't get to the Finder from another environment:

- Press Command-Shift-Esc when the Welcome dialog appears. Then enter either the computer owner's password or an administrator's name and password.
- If you have system access, choose the System Access workgroup when you log in.
- If you don't have system access and you need to go to the Finder regularly, ask your Macintosh Manager administrator to enable system access for your account.

Problems Client Users May Have

If users can't log in to the server:

Make sure the server has enough free disk space. Make sure the user's account hasn't been deleted or the password changed. Also, check the Basic pane of the Users pane to see if the user's login access has been disabled.

If a user's computer freezes:

If the computer is using system software earlier than Mac OS 9, make sure file sharing is turned off.

If a user can't get an application to open or work correctly:

- If "Enforce file level security for Mac OS 9 workstations" is enabled for this workgroup, some older applications may not function properly and report errors (see "Privileges Settings for Workgroups" on page 207).
- Some applications write to or create special files in places other than the Preferences folder in the System Folder. If a user is having trouble with an application, that could be the cause of the problem. Try putting the application folder (and all of its contents) in a folder called "Other Applications •" (the Option-8 bullet must be the last character in the name), in the client computer's Applications folder. (This folder is named "Applications [Mac OS 9]" on client computers with Mac OS 9.1 or later installed.) If an application is located in the Other Applications • folder, it can read, write, and open any plug-ins and files it needs to function.

If users can't see a volume they logged in to from the Chooser:

In the Panels environment, a mounted volume is not visible to users unless you select "Show volume on a panel" in the Volumes pane of the Workgroups pane.

If a user is having problems accessing his or her shared files:

Check whether the user belongs to more than one workgroup. Shared workgroup folders for all workgroups are located on the same server volume by default. However, if you store workgroup documents on different volumes, users may not be able to access all of their shared documents without changing workgroups. The user should upgrade to a newer version of AppleShare, or you should move the user's home directory to another volume using Server Admin.

If an application needs a file, but the user can't open the file:

You may not have given the user access to documents outside of the user's home directory. You can give the user temporary access to another folder. See the Privileges pane of the Workgroups pane.

If a workgroup data volume was created, but shared workgroup documents no longer show up in the Panels environment:

- Check to make sure the location of the Users folder has not changed. The Users folder is usually located at the top level of the server volume or workgroup data volume.
- Make sure the workgroup data volume you chose is the one where the shared documents are located.

If users can't drag and drop between applications:

For security reasons, most drag-and-drop features are not available. Use the Copy and Paste commands.

If the wrong application opens:

Each application is identified by its four-character creator ID, not by the application's filename. The wrong application may open if two applications have the same creator ID. Try rebuilding the client computer's desktop.

If a user cannot access his or her home directory:

- Make sure a home directory has been set up for the user in the Users & Groups module of Server Admin.
- Make sure the permissions for the home directory are set correctly.
- Check to make sure that the server where the user's home directory is located is running.

Where to Find More Information About Macintosh Manager

For additional information related to Macintosh Manager, try these resources:

- The AppleCare Web site provides several different information resources, including the Knowledge Base, a database of technical articles about product issues, usage, and implementation.
www.apple.com/support
- Discussion lists (Mac OS X Server and Macintosh Manager) let you exchange ideas and tips with other server administrators. You can sign up for a discussion list at the following Web address:
www.lists.apple.com

NetBoot

What Is NetBoot?

NetBoot allows network administrators to configure and update Mac OS 9 client computers instantly by simply updating the disk image on the server that clients start up from. Each disk image contains a System Folder that all clients can start up from. NetBoot ensures that the client systems are pristine images of what you set up on the server. Any changes you make on the server are automatically reflected on the client computers when they restart. You can use Macintosh Manager to provide authentication and a personalized work environment to any NetBoot client computer user.

Who Should Use NetBoot?

NetBoot is designed for any organization that uses Macintosh computers on a network. It helps educators bring technology into the classroom using low-cost, easy-to-manage computers like the iMac. NetBoot is ideal for educators who want to

- make more computers available to more students
- achieve technology goals under tight fiscal constraints
- reduce the cost of managing their computing infrastructure
- get the most out of existing technology resources

The NetBoot server is also ideal for businesses with Macintosh networks, particularly those that want to replace computers used primarily for data entry or word processing. These businesses can minimize their computer costs by using low-cost Macintosh hardware and taking advantage of the reduced administration requirements made possible by NetBoot.

Before You Set Up NetBoot

Before you set up NetBoot, be aware of the system requirements listed here:

Client computer requirements

- Mac OS 9.1 image that came with Mac OS X Server
- iMac, iBook, Power Macintosh G3 (Blue and White), Power Mac G4, Power Mac G4 Cube, PowerBook (FireWire), or PowerBook G4
- a minimum of 64 megabytes (MB) of random-access memory (RAM)

Each computer that you plan to start up from your Mac OS X Server needs an IP address to identify it as a unique device on the network. With this version of NetBoot, client computers can obtain their IP addresses using DHCP. (Only certain models of Macintosh computers can take advantage of this feature.) In the previous version of NetBoot, computers could only start up by acquiring their IP addresses using BootP (the bootstrap protocol). This version of NetBoot supports both DHCP and BootP. If the client computer supports it, DHCP is the preferred method of obtaining an IP address.

Before setting up your NetBoot server, you need to do the following:

- 1 Determine which of your computers can start up using DHCP and which ones need BootP. For more information, see “Client IP addresses” on page 248.
- 2 For computers that start up using BootP, determine the specific ranges of IP addresses you want to assign.
- 3 Read the next section, “Planning Your Network,” and gather the information you need to set up NetBoot. You can use the NetBoot Server Worksheet provided later in this chapter to organize the information.

Planning Your Network

As you plan your network, you need to gather information that you’ll use when you set up the network. You can write down this information on the NetBoot Server Worksheet, on page 253.

Step 1: Determine how many clients to connect to the server

The number of NetBoot client computers you can connect to your server depends on how your server is configured as well as a number of other factors. A NetBoot server that has this configuration can easily support 50 NetBoot client computers:

- Macintosh G3 or G4 computer with a 400 MHz or faster processor
- 256 MB of RAM
- Two or more 9 gigabyte (GB) hard disks (multiple hard disks allow NetBoot to more efficiently allocate resources).
- Gigabit Ethernet; four-port, 100Base-T or faster Ethernet card

If you want to use a server that has a different configuration, or you want to support more than 25 client computers, consider these factors:

- *Ethernet speed*: For optimum performance, 100Base-T or faster connections are highly recommended for both client computers and the server.
- *Hard disk capacity and number of NetBoot client computers*: The NetBoot server requires a certain amount of hard disk space for each client connected to it. The amount of space depends on the size and configuration of the system image.
- *Hard disk capacity and number of users*: If you have a large number of users, consider adding a separate file server to your network to store user documents. By default, if you're using Macintosh Manager, users' documents and preferences are stored on the NetBoot server, but any Apple Filing Protocol (AFP) server can store this information.
- *Location of server and client*: If NetBoot client computers require the use of BootP, they must be located on the same subnet as the server, and there can be only one BootP server on that subnet. However, there can be multiple NetBoot servers on the same subnet for serving images.
- *Number of Ethernet ports on the server*: If you're using four-port, 100Base-T cards, distributing NetBoot clients over multiple Ethernet ports on your server offers a performance advantage. You can add ports by adding Ethernet cards, or by using several ports on a multiport Ethernet card. Each port must serve a distinct segment.

Step 2: Gather information for the NetBoot Setup Assistant

You need the information listed in this section for each Ethernet port you plan to use for NetBoot clients. As you gather the information, write it on the NetBoot Server Worksheet, on page 253.

If you purchased your software with a server, the server may have up to five Ethernet ports. One port is the built-in Ethernet port that comes with your server. Other ports are on Ethernet cards installed in your server. The number of ports you have depends on the configuration of your server. The connection from the server to the NetBoot clients should be 100Base-T Ethernet or faster.

Port IP addresses and subnet mask

Each Ethernet port you use for NetBoot clients must have an IP address and a subnet mask. You should use a subnet mask that restricts local traffic to the IP addresses of the NetBoot clients that are connected to this port.

Client IP addresses

Determine which NetBoot clients can use DHCP and which cannot. These Macintosh computers are known to work with DHCP:

- all slot loading iMac computers
- all iBook computers
- all Power Mac G4 computers
- all Power Mac G4 Cube computers
- all FireWire PowerBook computers
- all PowerBook G4 computers

For other models of Macintosh, you may need to run the latest Firmware Update (available at the Apple Web site) to enable this capability or to determine whether the computer has the capability. (The updater displays a message if the computer doesn't require updating.)

- *For clients that use DHCP:*

If the client computer can use DHCP, you don't need to enter an IP address for those computers in the NetBoot Server Worksheet, unless there is no DHCP server on the same subnet as the computers.

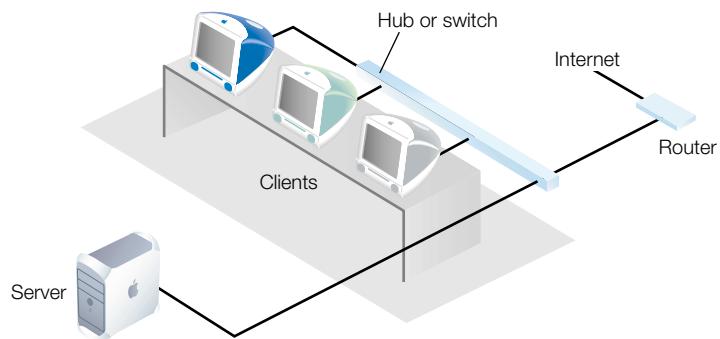
- *For clients that use BootP:*

For NetBoot clients connected to each port that uses BootP, you need to supply one or more ranges of IP addresses. You need to allow at least one IP address per computer, but it's best if you allocate a few extra to accommodate expansion.

IP routing information

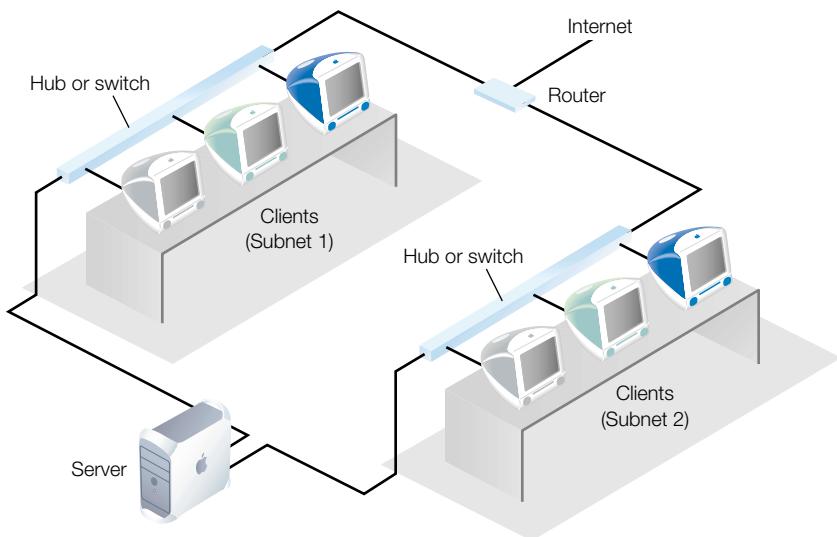
The IP routing information you provide to the NetBoot Setup Assistant depends on the configuration of your network.

In this case, the server is a peer of NetBoot clients on a single subnet—each is connected directly to the router. If this is your configuration, select Peer in the IP Routing for NetBoot Clients pane of the NetBoot Setup Assistant. For “Router IP address,” enter the IP address of the router.



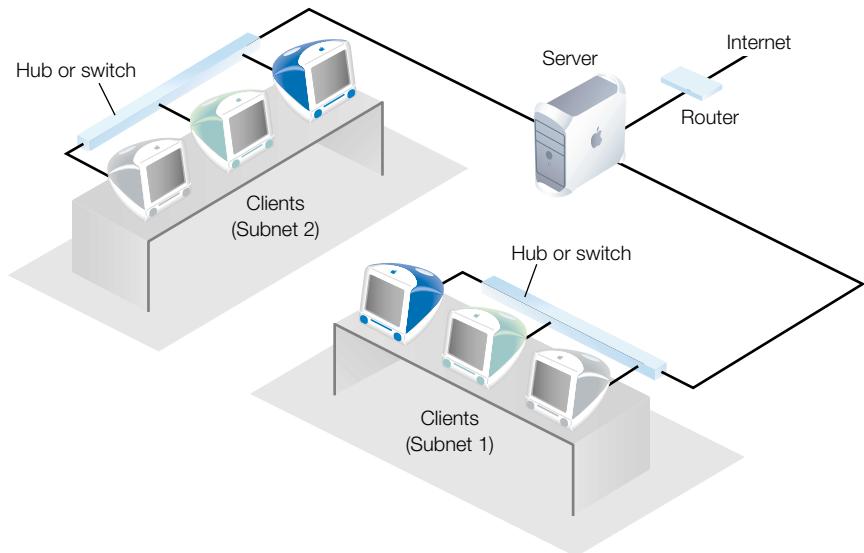
NetBoot clients are connected directly to the router.

The configuration below is similar to the previous one, except there are two NetBoot client subnets. Each subnet is connected to a different port on the router and a different port on the server. If this is your configuration, select Peer in the IP Routing for NetBoot Clients pane of the NetBoot Setup Assistant. For “Router IP address,” enter the IP address for the router port you connect to that subnet.



NetBoot clients are connected directly to the router.

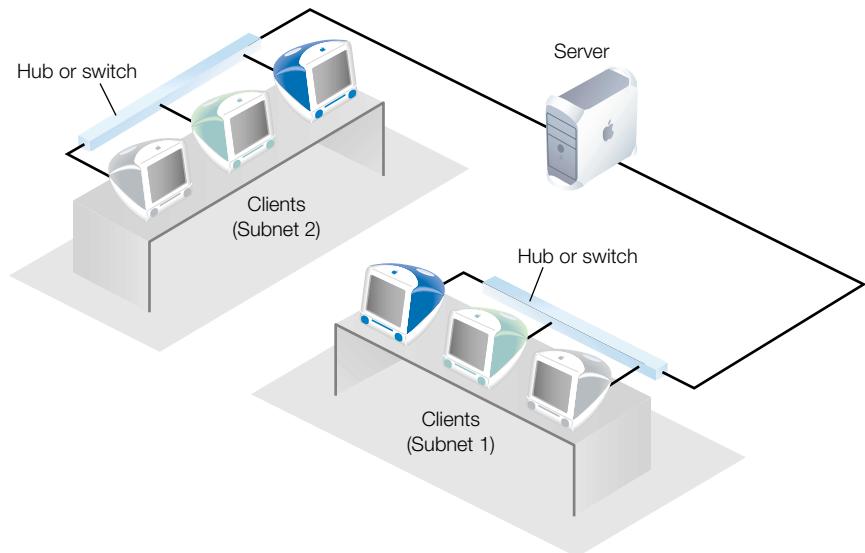
In this configuration, the server acts as a router to one or more NetBoot client subnets. If this is your configuration, select Gateway in the IP Routing for NetBoot Clients pane of the NetBoot Setup Assistant. You do not need to provide a router address.



The server is a gateway to the router.

Note: For clients to have access to the Internet, routing tables need to be updated to show that the server acts as a gateway for the client subnet. You need to make a separate entry for each client subnet. You use software that came with your router to make changes to the routing table.

If this is your configuration, select Gateway in the IP Routing Configuration pane of the NetBoot Setup Assistant. You don't need to provide a router IP address.



No router—NetBoot clients are isolated from the Internet.

NetBoot Server Worksheet

You need to provide the following information for each Ethernet port. The number of ports you have depends on the configuration of your server.

NetBoot port planning			
Specify the following information using the IP address format (for example, 124.50.66.93)			
Built-in Ethernet port		Ethernet card port 3	
IP Address:	IP Address:
Subnet Mask:	Subnet Mask:
Router Address:	Router Address:
BootP Address	BEGIN	BootP Address	BEGIN
Range (if needed):	END	Range (if needed):	END
Server is Peer or Gateway?	<input type="checkbox"/> Peer <input type="checkbox"/> Gateway	Server is Peer or Gateway?	<input type="checkbox"/> Peer <input type="checkbox"/> Gateway
Ethernet card port 1		Ethernet card port 4	
IP Address:	IP Address:
Subnet Mask:	Subnet Mask:
Router Address:	Router Address:
BootP Address	BEGIN	BootP Address	BEGIN
Range (if needed):	END	Range (if needed):	END
Server is Peer or Gateway?	<input type="checkbox"/> Peer <input type="checkbox"/> Gateway	Server is Peer or Gateway?	<input type="checkbox"/> Peer <input type="checkbox"/> Gateway
Ethernet card port 2			
IP Address:		
Subnet Mask:		
Router Address:		
BootP Address	BEGIN		
Range (if needed):	END		
Server is Peer or Gateway?	<input type="checkbox"/> Peer <input type="checkbox"/> Gateway		

Setting Up NetBoot Server Software for the First Time

If you have not read the section “Planning Your Network” on page 246 and filled out the NetBoot Server Worksheet, you should do so now before you proceed. You need to have this information handy when you use the NetBoot Setup Assistant.

Step 1: Install NetBoot server software (optional)

If you purchased your software with a server, the NetBoot server software is already installed. You can skip this step and go on to step 2.

If you purchased your Mac OS X Server software without hardware, you need to install the NetBoot server software, which is on a separate CD that came with your Mac OS X Server software. You must install NetBoot server software on a computer that already has Mac OS X Server software installed and set up.

To install NetBoot server software, follow these steps:

- 1** Insert the NetBoot CD in your computer’s CD-ROM drive.
- 2** Double-click the NetBoot CD icon.
- 3** Double-click NetBoot.pkg.
- 4** Follow the onscreen instructions. Use the administrator password you set up when you used the Mac OS X Server Setup Assistant.

The Installer guides you through the steps necessary to install the software.

Step 2: Use the NetBoot Setup Assistant

If you just installed the NetBoot software, the Setup Assistant should open automatically. If the Assistant isn’t open, follow these steps to open it:

- 1** Log in to the Mac OS X Server as the administrator. Use the administrator password you set up when you used the Mac OS X Server Setup Assistant.
- 2** Double-click Assistant in the /Applications/Utilities directory.
- 3** When the Assistant window opens, double-click NetBoot Setup Assistant.
- 4** Follow the onscreen instructions.

The Setup Assistant guides you through the steps necessary to set up the software. To learn more about each step, click the Tell Me More button in the window.

If you need to change any setup information in the future, you can use the NetBoot Setup Assistant.

Step 3: Set up Macintosh Manager

If you plan to use Macintosh Manager to provide authentication and personalized work environments for NetBoot client users, make sure it is set up and users have been imported from the Mac OS X Server Users & Groups database. Set up the Macintosh Manager workgroups and settings you need (see Chapter 10, “Macintosh Management Service,” on page 195). Make sure you have at least one Macintosh Manager administrator user assigned to the System Access workgroup.

Step 4: Start up a NetBoot client computer

Any Mac OS computer that can start up from a NetBoot server can be a NetBoot client computer.

If your computer’s firmware needs to be updated, update it now. For more information, see the Apple Web site.

To start up a NetBoot client computer, follow these steps:

- 1** Connect the client computer to the network.
- 2** Hold down the N key while you turn on the client computer.

The computer looks for a NetBoot server. It may take several seconds for the client computer to find the server and start up. If the computer doesn’t start up after more than a minute, see “Solving Problems With NetBoot” on page 261.

Once the computer has started up, you see a volume named NetBoot HD.

Open the Startup Disk control panel and choose Network Disk.

The next time you start up the computer, you do not need to press the N key. Once a computer has started up from the NetBoot server, it will always start up from the NetBoot server unless there is a problem (such as that the server is turned off) or you change the startup disk in the Startup Disk control panel.

Using NetBoot Desktop Admin

The NetBoot HD volume you see when you start up a NetBoot client computer is a read-only disk image, which you cannot change. To install new software on the disk image or change how the system is configured, you use the NetBoot Desktop Admin application to create a copy of the image that you can change. When you finish, NetBoot Desktop Admin replaces the existing disk image with the one you changed.

Installing Software or Changing the Disk Image

To install software or change the NetBoot HD disk image, you need to start up from a NetBoot client computer, connect to the NetBoot server volume, and open the NetBoot Desktop Admin program, as described in the following steps. Your changes are not available to you or other users until after the NetBoot client computer running NetBoot Desktop Admin restarts the last time.

Before you start, you need the following information:

- Name and password of a user with read and write access privileges to the NetBoot server volume (for example, the administrator of the Mac OS X Server)

Note: If you are using Macintosh Manager with NetBoot client computers, each time you start or restart the client computer, you need to log in as a Macintosh Manager administrator who belongs to the System Access workgroup.

To install software or change the NetBoot HD disk image:

- 1 Log in to the server volume as a user with read and write access privileges (for example, the administrator of the Mac OS X Server), and open the NetBoot Desktop Admin application.

Unless you've moved it, the application is in the NetBoot Desktop Admin folder, which is in the Admin folder on the NetBoot server.

- 2 If you are installing new software, increase the size of the disk image (if necessary).

Be sure the disk image has enough space for the software you want to install. However, increase the size of an image only as much as needed. You cannot reduce the size of an image without reverting to a backup copy.

Note: If you are installing a new version of the Mac OS, increase the size of the NetBoot HD disk image by at least 50 MB.

- 3 Click Make Private Copy.

NetBoot Desktop Admin creates a copy of the disk image. This may take several minutes, and you should not interrupt the process. When it finishes, your NetBoot client computer restarts automatically.

Important Because the copy of a disk image is associated with the NetBoot client computer you used to create it, you must make the changes to the image using the same computer. If you change computers, you will not be able to see the changes you have made and your changes will not be available to users. In addition, you increase the risk of unauthorized users making changes to the disk image.

- 4 Install the software or make changes to the system configuration.

If you are installing software, follow the installation instructions that came with the software. If necessary, restart the computer.

If you install an application, open it. Doing so lets you enter a registration number, if necessary. If you don't enter the number now, every time users open the application they will need to enter the registration number. In addition, most applications create a preferences file in the System Folder. If you don't open the application, users may not be able to open the application because the preferences won't exist.

- 5 Be sure there aren't any files in the Trash that you want to save. (The Trash is emptied automatically after the next step.)

Note: If you cannot empty the Trash because it contains files that are in use, you may need to restart the computer.

- 6 Open the NetBoot Desktop Admin application, then click Save or Discard. The computer restarts automatically.

If you need to make other changes, click Quit and return to step 5.

- 7 Start the NetBoot client computer again, then open the NetBoot Desktop Admin application.

If you want to keep a backup copy of the old disk image, leave the "Keep previous disks as backup" option selected. Backup copies are stored in the Backup Images folder in the Shared Images folder on the NetBoot server.

- 8 If you clicked Save in step 6, click Restart. Otherwise, click OK.

If you click Restart, NetBoot Desktop Admin saves your changes, deletes the old disk image, then restarts the computer. Changes are available the next time a NetBoot client computer restarts. If you click OK, NetBoot Desktop Admin deletes the old disk image.

NetBoot Strategies and Tips

Improving NetBoot Performance

A number of factors affect NetBoot client performance. You can adjust some factors to decrease NetBoot client startup time, improve client performance, and increase the number of clients you can support. You can also make adjustments to increase network and server performance.

The factors you adjust to optimize network performance depends on your network setup. The best strategy is to identify the areas that will have the most impact and change them first. You may find that implementing just a few of the changes suggested here can greatly improve the user experience.

Network Performance Factors

- You get the best performance from a 100Base-T or faster Ethernet network, in which the server and the clients are on the same segment or hub. At a minimum, 10Base-T “switched” Ethernet can be used for the client computers, provided that the server has a 100Base-T or faster connection to the 10Base-T switched network. Although NetBoot works with a 10Base-T switched Ethernet network, 100Base-T or faster connections offer optimum performance.
- Analyze usage patterns before setting up a NetBoot network so you can determine how many client computers to connect to each segment or hub. If you expect heavy usage, you may need to split up some services (such as Apple file service or Macintosh Manager) among multiple servers.
- It is always better to use switches, not hubs, in a NetBoot environment.

NetBoot and AirPort

The use of AirPort wireless technology with NetBoot clients is *not* supported by Apple.

Server Performance Factors

- In a single-server network, every client on the network uses the same server to start up, access virtual memory, and get access to files and applications. This puts a great demand on the server’s hard disk and on the network. Increasing the amount of RAM installed in the server to at least 256 MB can help reduce the load on the server’s hard disk.
- The server’s processor speed is also important, especially in a single-server network. Always use the fastest supported computer available as the server.
- If you are using Macintosh Manager, adding another hard disk can also help to improve performance because the Macintosh Management server must give access to the same server volume to many clients simultaneously.
- Using another Apple Filing Protocol (AFP)-compatible server for document storage can further reduce the server’s workload.
- You may be tempted to rearrange the system files associated with NetBoot and Macintosh Manager. However, doing this incorrectly may make your server unusable. Rearranging system files is *not* recommended.

Client Performance Factors

- Perhaps the most reliable way to improve performance is to increase the RAM installed in each client computer. This cuts down on the client's need to use virtual memory and allows the client to make greater use of the memory cache.
- You can also boost client performance by setting client computers to use virtual memory from the client hard disk, instead of over the network (the default). This can reduce network traffic and the load on the server's hard disk and offers better client performance, especially when opening applications. To allow clients to use virtual memory from the client hard disk, use NetBoot Desktop Admin to change the system image on the server, as described in "Installing Software or Changing the Disk Image" on page 256. Once you have made a copy of the image that you can modify and then restarted, open the Memory control panel and select the local hard disk in the Virtual Memory area. After you change the virtual memory settings, make the new system image "shareable" again using NetBoot Desktop Admin. Make sure that all of the NetBoot clients have the same local hard disk name.
- If a client has a lot of RAM installed, you may want to consider turning off virtual memory. Note, however, that in Mac OS 9, virtual memory is turned on by default and is generally recommended.
- If you are using Macintosh Manager, it allows you to save preferences files for each individual user. These files are stored on the server. The more preferences you save, the longer it will take for client computers to load them when a user logs in. If you are encountering long delays immediately after login, consider reducing the number of preferences you are saving in Macintosh Manager.

Most importantly, do not save a user's Web browser cache. Browser caches can grow quickly in an environment where Internet browsers are heavily used. Setting Macintosh Manager not to save the browser cache eliminates the transfer of these large files between the server and the client, thus reducing startup times after login dramatically.

Performance Summary

For best performance, follow these tips:

- Always use at least a 100Base-T or faster Ethernet connection from the server to the network where the NetBoot clients reside.
- The minimum recommended connection from the client to the network is switched full-duplex 10Base-T Ethernet. A 100Base-T or faster Ethernet full- or half-duplex connection is recommended. Ethernet switches should be configured to support automatic negotiation of the duplex mode.
- Choose server, network, and client configurations that support the usage patterns of your users.
- Add more servers to your network, and consider dividing NetBoot, Macintosh Manager, and Apple file service among different servers.

- Install additional RAM in the server to reduce the load on the server's hard disk.
- Add hard disks to your server to enhance performance.
- Use the fastest computer available as the server, especially in a single-server network.
- Install additional RAM in NetBoot clients to reduce the use of virtual memory across the network.
- Set up NetBoot clients to use virtual memory from the local hard disk.
- Reduce the number of preferences Macintosh Manager saves for users.
- Do not save Web browser caches.

Inside NetBoot

While earlier versions of NetBoot included both a System disk image and an Application disk image, the NetBoot server now requires only one image, the NetBoot HD disk image. You can install applications in the NetBoot HD disk image, or you can continue to use the Application disk image. You can also continue to use NetBoot Desktop Admin to make changes to the Application disk image.

Important Because NetBoot client computers must use the Mac OS 9.1 image supplied by the NetBoot server, each NetBoot client computer must be licensed to operate Mac OS 9.1. This means that Mac OS 9.1 must have been included with the client computer, or you must have purchased a license for it. The Mac OS X Server and NetBoot server license agreements do not include any Mac OS licenses.

A NetBoot client computer using Mac OS 9 requires 64 MB of memory. If a NetBoot client computer does not have this much memory, use NetBoot Desktop Admin to increase virtual memory to equal or exceed this amount. To increase virtual memory, use the Memory control panel after restarting from the private copy of the NetBoot HD image. If at all possible, follow the recommendation to allocate virtual memory on the client computer's local hard disk (see "Client Performance Factors" on page 259).

Solving Problems With NetBoot

If a NetBoot client computer won't start up:

- Sometimes a computer may not start up immediately because other computers are putting a heavy demand on the network. Wait a few minutes and try starting up again.
- Make sure that all the cables are properly connected, and that the computer and server are getting power. See the troubleshooting information that came with the client computer for more information.
- Check that one end of the Ethernet cable is plugged into the Ethernet port on the computer and the other end is plugged into a working Ethernet connector on a switch or hub.
- Make sure you haven't exceeded the number of IP addresses assigned to your network.
- If you installed memory or an expansion card in the client computer, make sure it is installed properly.
- If the server has more than one Ethernet card, or you are using more than one port on a multiport Ethernet card, check to see if other computers using the same card or port can start up. If they can't, check to be sure the Ethernet port you set up on the server is the same port the client computer is connected to. It's easy to mistake Ethernet port 1 for Ethernet port 4 on a multiport card. On the cards that come preinstalled in Macintosh servers, the ports are numbered 4, 3, 2, 1 (from left to right), if you're looking at the back of the computer.
- If the computer has a local hard disk with a System Folder on it, disconnect the Ethernet cable and try to start up the computer from the local hard disk. Then reconnect the Ethernet cable and try to start up the computer from the network.

If you are using Macintosh Manager and a user can't log in to a NetBoot client:

- Check to see if the user can log in to other computers. If the user can log in to other computers, then the computer the user can't log in to may be connected to a Macintosh Manager server the user does not have an account on. If there is more than one Macintosh Manager server, make sure the user has selected a server on which he or she has an account.
- Open Macintosh Manager and make sure the user is a member of at least one workgroup.
- Open Macintosh Manager and reset the user's password.

Network Services

What Are Network Services?

Network services control Internet communications on a TCP/IP network. Mac OS X Server includes these network services:

- Service Location Protocol (SLP) Directory Agent (DA) service
- Dynamic Host Configuration Protocol (DHCP) service
- Domain Name System (DNS) service
- IP filter service

You use network services to administer your company's IP addresses, organize network resources, manage domain names, and set up IP filters to block unwanted Internet connections. If you have a medium- to large-size network, network services will probably benefit you.

This chapter includes a section for each of the four network services offered with Mac OS X Server. In each section, you'll find information you need to know to better understand how the service works, what features it offers, and how to set up the service for the first time. You'll also find illustrations of the main settings panes and information about the options in these panes. Most sections also include information for more advanced network administrators, and places to look for additional information.

Service Location Protocol (SLP) Directory Agent (DA) Service

SLP DA service provides structure to the services (or resources) available on a network and gives users easy access to them. Anything that can be accessed using a URL—including file servers, WebDAV servers, NFS servers, printers, and personal Web servers—can be a network service.

When a service is added to your network, it uses SLP to “register” itself—or make its presence known and identify the service it provides—on the network. You don’t have to configure it manually. When a client computer needs to locate a network service, it uses SLP to look for services of that type. All registered services that match the client computer’s request are displayed to the user, who can then choose which one to use.

SLP Directory Agent (DA) is an improvement on basic SLP, storing registered network services in a central repository. You can set up a directory agent to keep track of services for one or more *scopes* (groups of services). When a client computer looks for network services, the directory agent for the scope in which the client computer is located responds with a list of available services. Because a client computer only needs to look locally for services, network traffic is kept to a minimum and users can connect to network services more quickly.

Who Should Use SLP DA Service?

Normally, SLP service sends requests to all SLP services on a network, which can substantially increase network traffic. If you have a large network, SLP communications can slow network performance and increase the amount of time users must wait to locate network services. You can improve SLP performance by setting up SLP DA service. You should also consider setting up more than one directory agent, so client computers can contact the directory agent closest to them for services, and services can be registered with more than one directory agent.

Before You Set Up SLP DA Service

Before you set up SLP DA service, read this section to learn about defining scopes and making sure of client and router compatibility.

Defining Scopes

To define scopes, you need to decide how you want to organize the computers on your network. A scope can be a logical grouping of computers, such as all computers used by the production department; or a physical grouping, such as all computers located on the first floor. You can define a scope as part or all of your network. Even if you don’t plan to divide your network into scopes, you still need to set up at least one scope to use SLP DA service.

Client and Router Compatibility

Your client computers must be using Mac OS 9.1 or later to use SLP DA service. Versions of SLP on Mac OS 9.0 will continue to use IP multicast. If your network uses routers that are not capable of IP multicast, you will need to upgrade them or set up tunneling. See the documentation that came with your routers for information on tunneling.

Setting Up SLP DA Service for the First Time

Follow the steps below to set up SLP DA for the first time. If you need more information to perform any of these tasks, see the onscreen help.

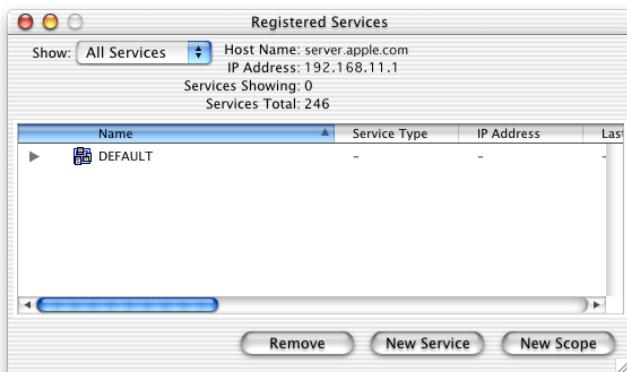
Step 1: Configure logging settings

You can log events to help you monitor SLP DA activity. If problems occur, or if you want to improve service performance, the entries in the log can provide important diagnostic information. SLP DA service errors are logged automatically, but you can configure the service to log other types of events as well.

To configure logging settings, click the Network tab, then click SLP Service and choose Configure SLP DA. Then choose the settings you want. You can find more information about the settings in “SLP DA Service Settings” on page 267.

Step 2: Create scopes for your network

To create scopes, click SLP Service and choose Show Registered Services. The Registered Services window appears.



Click New Scope and type the name of the scope you are creating in the Add Scope dialog, shown below. SLP DA service converts the name you type to the correct format and adds it to the list in the Registered Services window.



Step 3: Assign network services to each scope

Once you've created a scope, you can assign network services to it. In the Registered Services window, click New Service. In the Add Proxied Service dialog (shown below), you can choose the scope and add the service you want. For more information about the Add Proxied Service dialog, see "Registered Services Settings" on page 268.



Step 4: Start SLP DA service

To start SLP DA service, click SLP Service and choose Start SLP DA. When the service is turned on, a globe appears on the service icon. As services on the network register with the directory agent, they appear in the Registered Services window under the appropriate scope.

SLP DA Service Settings

Configure SLP DA Settings

The Configure SLP window lets you choose logging settings for SLP DA service. To access this window, click the Network tab, then click SLP Service and choose Configure SLP DA.



Registrations and Deregistrations

Select this option if you want to log when services are registered and deregistered. Services reregister themselves periodically, and you can register services manually. If a service hasn't been in contact for a certain period of time, the service is deregistered.

Expirations

Select this option if you only want to log when services are deregistered. Selecting this option creates fewer log entries than logging both registrations and deregistrations.

Service Requests

Select this option if you want to log each time a client computer requests a network service. Since service requests happen frequently on a network, selecting this option could create a large number of log entries.

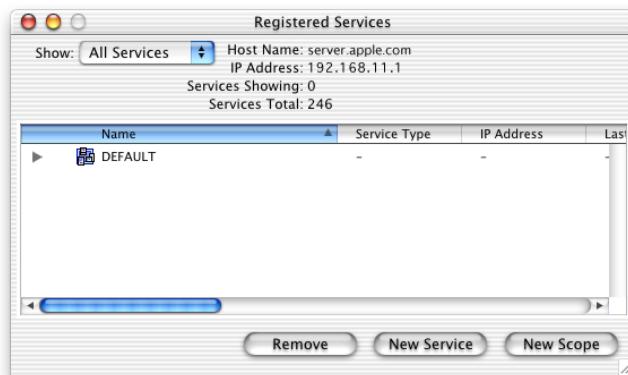
Directory Agent Info Requests

Select this option if you want to log each time client computers look for or request information about the directory agent. This option could also create a large number of log entries.

Registered Services Settings

The Registered Services window lets you view scopes and registered services, and create and manage scopes and services. At the top of the window you can see the host name and IP address of the Mac OS X Server to which you are connected, the number of services showing, and the total number of registered services.

To access the Registered Services window, click SLP Service and choose Show Registered Services.



The list shows all the scopes defined on this server. Click the triangle next to a scope to see the services registered to it.

Show

Choose the type of services you want to see from the Show pop-up menu. You can choose All Services or choose from the other types of available services.

Remove

Select a scope or service in the list and click Remove to deregister a service or eliminate a scope. Deregistering a non-local service may only be temporary if that service reregisters itself with the directory agent.

New Scope

Click New Scope to create a new scope.

New Service

Click New Service to register a service with SLP DA and assign it to the selected scope. The Add Proxied Service dialog, below, appears.



Scope

Choose the scope to which you want to add a service.

URL

Type the URL for the service.

Attribute List

Type information about the service in this field. Attributes are properties that describe the service, such as the name of the service, the number of pages that can be printed per minute, and so on. This is an optional field, and you shouldn't enter anything here unless you know the correct format to use. For more information about attributes, see “Using the Attributes List” on page 270.

SLP DA Service Strategies and Tips

If you are an advanced administrator, SLP DA service has some additional features that you may want to know about and use.

Working With Logs

SLP DA service log entries are stored in the system log. To access the system log, click the General tab in Server Admin, then click Log Viewer and choose System Software. Choose System Log from the pop-up menu. The system log may contain hundreds of entries, so look for “slpd” to find SLP DA service events.

When you configure logging, you choose the types of events you want to log. The table below shows the error string associated with each type of event in the log.

Error string	SLP DA service event
REG	Registrations and deregistrations
EXP	Expirations (services that have been deregistered)
SR	Service requests
DA	Directory agent info requests
ERR	SLP errors

Logging Debugging Messages

In addition to the logging options described earlier in this chapter, you can choose to log all events, including debugging messages. This feature is useful to advanced system administrators. To log debugging messages, click SLP Service, then hold down the Option key and choose Configure SLP DA. You'll see the option All Messages in the Configure SLP window.



Using the Attributes List

Services may advertise their presence on the network along with a list of attributes. These attributes are listed as a string encoding that follows a specific format. Directory agents use the attributes list to help match client requests with appropriate services.

Here is an example of an attributes list for a network printer named Amazon. It's an LPR printer located in the Research scope. The attributes list entered by the administrator might look like this:

```
(Name=Amazon),(Description=For research dept only),(Protocol=LPR),(location-description=bldg 6),(media-size=na-letter),(resolution=res-600),x-OK
```

If you create an attributes list for a service, the directory agent must scan it when it's looking for services. So, if you create an attributes list that is incorrectly formatted, you could inadvertently block the directory agent from using a service.

Dynamic Host Configuration Protocol (DHCP) Service

DHCP service lets you administer and distribute IP addresses to client computers from your server. When you configure the DHCP server, you assign a block of IP addresses that can be made available to clients. Each time a client computer starts up, it looks for a DHCP server (you can have more than one on your network), then it requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a “lease period” (the length of time the client computer can use the address) and configuration information.

You can use the DHCP module in Server Admin to

- configure and administer DHCP service
- create and administer subnets
- configure DNS and NetInfo options for client computers
- view DHCP and NetBoot client computers

Who Should Use DHCP Service?

If your organization has more clients than IP addresses, you will benefit from using DHCP service. IP addresses are assigned on an as-needed basis, and when they are not needed, they are available for use by other clients. You can use a combination of static and dynamic IP addresses for your network if you need to. Read the next section for more information about static and dynamic allocation of IP addresses.

Larger organizations may also benefit from some of the other features DHCP service provides, such as being able to set DNS and NetInfo options for client computers.

You may not need to use DHCP service if you have a simple network with enough IP addresses for your clients. You can use one of the methods described later in this chapter to assign static IP addresses to all your network clients.

Before You Set Up DHCP Service

Before you set up DHCP service, read this section for information about creating subnets, assigning static and dynamic IP addresses, locating your server on the network, and avoiding reserved IP addresses.

Creating Subnets

Subnets are groupings of client computers on the same network that simplify administration. You can organize subnets any way that is useful to you. For example, you can create subnets for different groups within your organization, or different floors of a building. Once you have grouped client computers into subnets, you can configure options for all the computers in a subnet at one time instead of setting options for individual client computers.

Assigning IP Addresses Dynamically

With dynamic allocation, an IP address is assigned for a limited period of time (the *lease period*) or until the client computer doesn't need the IP address, whichever comes first. By using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

Using Static IP Addresses

Static IP addresses are assigned to a computer or device once and then do not change. You may want to assign static IP addresses to computers that must have a continuous Internet presence, such as a Web server. Other devices that need to be available to network users on an ongoing basis, such as printers, may also benefit from static IP addresses.

Server Admin does not provide a way to configure the bootp daemon to assign static IP addresses using the BootP protocol (the protocol underlying DHCP). To do so, you can use the NetInfo Manager application in Mac OS X to create the appropriate properties in the local NetInfo database.

Locating the DHCP Server

When a client computer looks for a DHCP server, it broadcasts a message. If your DHCP server is on a different subnet from the client computer, you must make sure the routers that connect your subnets can forward the client broadcasts and the DHCP server responses. If you have a relay agent program on your network that can relay BootP communications, it will work for DHCP. If you don't have a relay program, you need to place the DHCP server on the same subnet as your clients.

Assigning Reserved IP Addresses

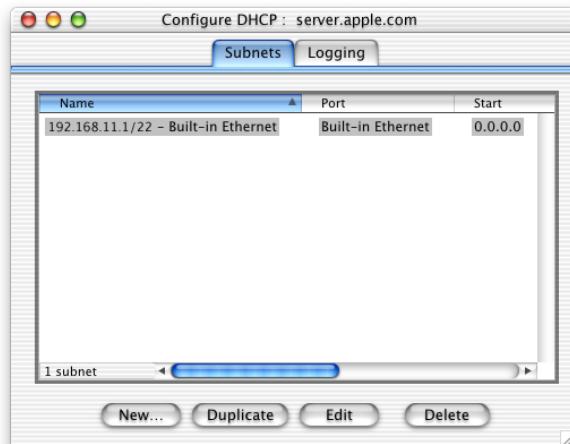
Certain IP addresses can't be assigned to individual hosts. These include addresses reserved for loopback and addresses reserved for use in multicasting. Your ISP will not assign such addresses to you. If you try to configure DHCP to use such addresses, you will be warned that the addresses are invalid, and will need to enter valid addresses.

Setting Up DHCP Service for the First Time

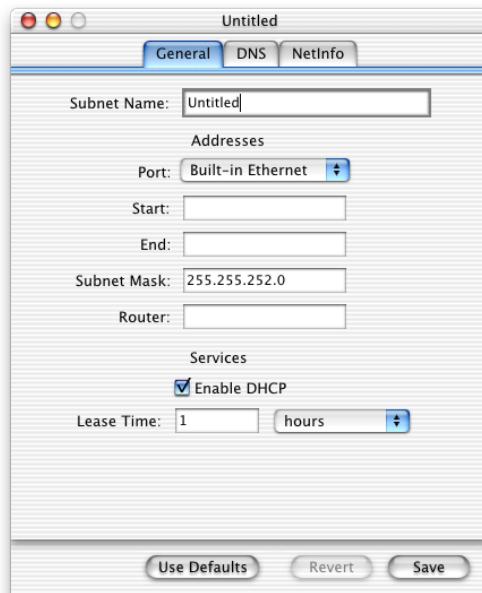
If you used the Setup Assistant to configure ports on your server when you installed Mac OS X Server, some DHCP information is already configured. You still need to follow the steps in this section to finish configuring DHCP service. You can find more information about the settings choices for each step in the next section, "DHCP Service Settings."

Step 1: Create subnets

In Server Admin, click the Network tab, then click DHCP/NetBoot and choose Configure DHCP. If you configured ports in the Setup Assistant, you see the port information in the Subnets pane. (The list of subnet address ranges shown is extracted from the host's local NetInfo database; it is initially set to one subnet address range for each active Ethernet port.)



Click New to create new subnets, or choose an existing subnet and click Edit.



In the General pane of the subnet settings window, you need to set a range of IP addresses for each subnet, and specify the router address. If you don't use a router on your network, enter your server's IP address in the Router field. When you click Enable DHCP, you can choose a lease time for the IP address.

Click the DNS and NetInfo tabs to set options for your client computers. Default settings for the server, if they exist, already appear in each pane. Configuring the options in these panes provides a starting point for client computers when DHCP service is turned on.

Step 2: Set up logs for DHCP service

You can log DHCP activity and errors to help you monitor requests and identify problems with your server.

DHCP service records diagnostic messages in the system log file. To keep this file from growing too large, you can suppress most messages by selecting "serious errors only (quiet)" in the Logging pane of the Configure DHCP window.

Step 3: Start DHCP service

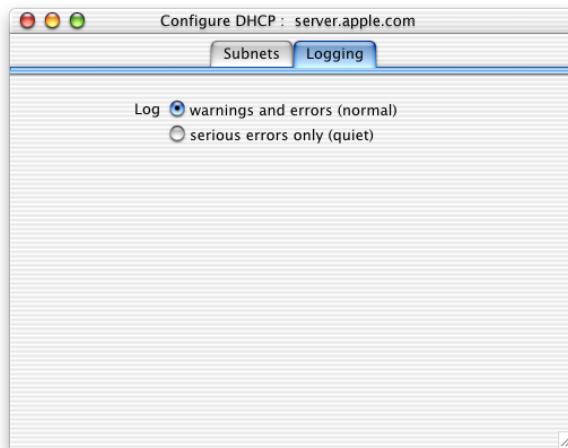
Click DHCP/NetBoot and choose Start DHCP. If the server successfully starts up, the menu item changes to Stop DHCP, and a globe appears on the DHCP/NetBoot icon.

DHCP Service Settings

To access the DHCP settings, click the Network tab in Server Admin, then click DHCP/NetBoot and choose Configure DHCP. The Configure DHCP window has two panes: Subnets and Logging.

Logging Settings

Click the Logging tab in the Configure DHCP window to access the logging settings.



Log warnings and errors only (normal)

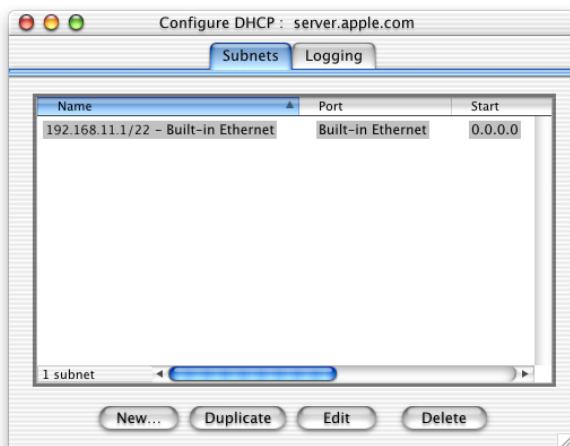
Warnings can alert you to conditions in which data is inconsistent, but the DHCP server is still able to operate.

Log serious errors only (quiet)

Serious errors indicate conditions for which you need to take immediate action (for example, if the DHCP server can't start up).

Subnets Settings

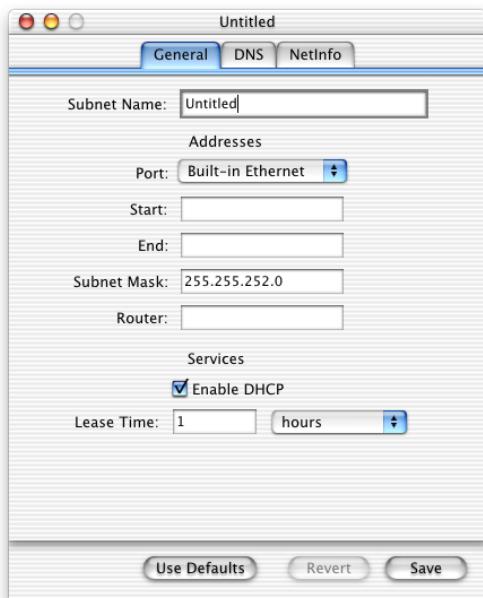
Click the Subnets tab in the Configure DHCP window to access the subnet settings.



Click New, or select a subnet in the list and click Edit to access the subnet settings window, which has three panes: General, NetInfo, and DNS. The settings in each of these panes are described in the following sections.

Subnet General Settings

The General pane of the subnet settings window lets you set general options for the subnet, such as the port the subnet uses and the subnet name.



Subnet Name

Enter a name for the subnet. You should choose a name that helps you remember the purpose of the subnet, such as German Lab or Fifth Floor.

Port

Choose a port for this subnet from the pop-up menu. The menu contains the number of network interfaces installed on your server.

Start and End

Enter the IP addresses that you want this subnet address range to start and end with. You can set up a second block of addresses for this subnet by creating a new subnet address range. If a subnet is assigned multiple ranges, the ranges can't overlap.

Subnet Mask

Enter the subnet mask for this range of IP addresses. Click Use Defaults to have the DHCP server automatically set a subnet mask.

Router

A port's address range is defined in the server's Network preferences. If the subnet uses another port for communication outside the subnet, you must enter the router address.

Enable DHCP

Click Enable DHCP if you want clients in this subnet to use DHCP to contact services. Client computers receive whatever IP address is available when they start up.

Lease Time

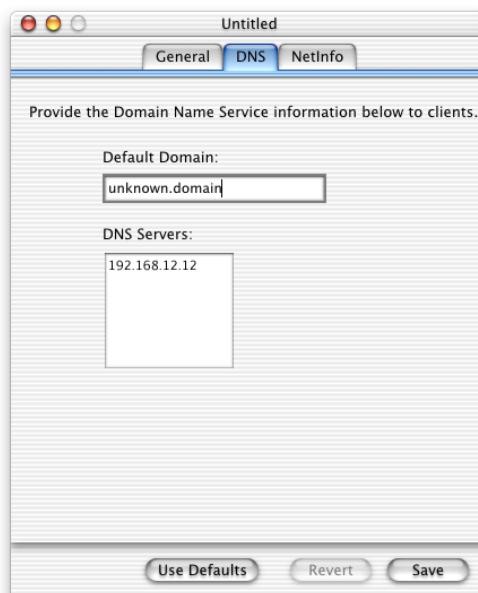
Enter a number in this window and choose a value from the pop-up menu to limit the amount of time a client computer can use an IP address. Halfway through the lease, it's renegotiated if the address is still in use.

Use Defaults

Click this button to use the default subnet address range for this port. The default range includes all valid addresses for the port, based on its IP address and subnet mask.

Subnet DNS Settings

The DNS pane of the subnet settings window lets you specify the DNS information that will be provided to client computers in a subnet.



Default Domain

Enter the domain name associated with this subnet.

DNS Servers

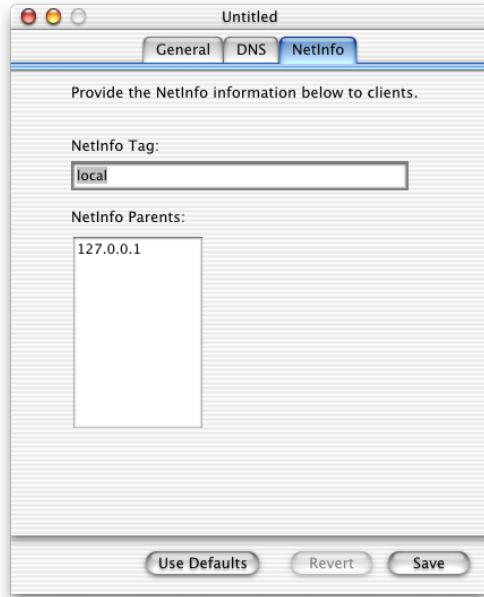
Enter the IP addresses of the servers that will provide DNS information to client computers in this subnet. You should list at least two DNS servers to ensure that network services aren't disrupted in case one server is unavailable. You can list up to three.

Use Defaults

If you click Use Defaults, DHCP service gets DNS information from a DNS lookup that supplies the domain name and default DNS servers.

Subnet NetInfo Settings

The NetInfo pane lets you "bind" client computers in a subnet to a particular NetInfo database, or domain. For more information about NetInfo, see Chapter 2, "Directory Services."



NetInfo Tag

Enter the name of the NetInfo domain that you want this subnet to contact for information. The name is a tag in the form of a text string; for example, "network."

NetInfo Parents

Enter an IP address for each server to which you want to bind this subnet. Binding to a parent server is useful if you want to allow client users to log in from different locations and still have access to the same information. You can have more than one parent for each subnet.

Use Defaults

Click this button to use the server's defaults.

DHCP Service Strategies and Tips

DHCP service provides some useful tools for monitoring DHCP and NetBoot client computers. You can view lists of DHCP and NetBoot clients, and you can check the system log for DHCP errors.

Viewing DHCP and NetBoot Client Lists

The DHCP and NetBoot client lists show snapshots of the clients in the database at a specific time. The lists are updated every five minutes, but you can also click Refresh to update them manually. In both lists, you can change the sort criteria by clicking column headings.

The DHCP Clients window gives the following information for each client:

- The IP address served to the client. Declined addresses are listed with “Declined” in the Time Left column.
- The number of days of lease time left, until the time is less than 24 hours; then the number of hours and minutes
- The DHCP client ID. This is usually, but not always, the same as the hardware address.
- The computer name
- The hardware address

The NetBoot Clients window gives the following information for each client:

- The path to the startup disk image used by the client
- The client's Ethernet address (from the TCP/IP control panel)
- The version of system software and the type of CPU

Viewing DHCP Log Entries

DHCP events are logged in the system log. To view this log, click the General tab in Server Admin, then click Log Viewer and choose System Software. Choose System Log from the pop-up menu. DHCP entries are preceded by “bootpd.”

Domain Name System (DNS) Service

When your clients want to connect to a network resource such as a Web or file server, they may want to request it by its domain name (such as www.example.com) rather than its IP address (such as 192.168.12.12). DNS is a distributed database that maps IP addresses to domain names, so your clients find the resource they requested.

A DNS server keeps a list of domain names and the IP addresses associated with each name. When a computer needs to find the IP address for a name, it sends a message to the DNS server (also known as a *name server*). The name server looks up the IP address and sends it back to the computer. If the name server doesn't have the IP address locally, it sends messages to other name servers on the Internet until the IP address is found.

Mac OS X Server uses Berkeley Internet Name Domain (BIND) for its implementation of DNS protocols. BIND is an open source implementation, and is used by the majority of name servers on the Internet.

Who Should Use DNS Service?

If you don't have an Internet service provider (ISP) who handles DNS service for your network and either of the following is true, you need to set up DNS service:

- You have a mail server on your network.
- You want to create subdomains within your primary domain.

Before You Set Up DNS Service

Read this section for information to consider if you're using DNS on your network. You should also have a thorough understanding of DNS before you attempt to set up your own DNS server. A good source of information about DNS is *DNS and BIND*, 3rd edition, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 2001).

Setting Up Multiple Name Servers

You should set up at least one primary name server and a secondary name server. That way, if the primary name server unexpectedly shuts down, the secondary name server can continue to provide service to your users. A secondary server gets its information from the primary server by moving all the information from the primary server periodically.

DNS servers in a domain normally cache DNS information from other servers, which also helps to ensure DNS services are available. DNS information is usually cached for a set time, referred to as a *time-to-live* (TTL) value. When a domain name/IP address pair has been cached longer than the TTL value, the entry is deleted from the name server's cache. (It's never deleted from the primary DNS server.)

Setting up DNS Service for the First Time

If you are using an external DNS name server and you entered its IP address in the Setup Assistant, you don't need to do anything else. If you are setting up your own DNS server, follow the steps in this section.

Step 1: Register your domain name

Domain name registration is managed by a central organization, InterNIC. InterNIC registration makes sure domain names are unique across the Internet. (See www.internic.net for more information.) If you don't register your domain name, your network won't be able to communicate over the Internet.

Once you register a domain name, you can create subdomains within it as long as you set up a DNS server on your network to keep track of the subdomain names and IP addresses.

For example, Apple is in the ".com" domain, and has subdomains "corp" (corp.apple.com) and "austin" (austin.apple.com). The DNS server for Apple keeps track of information for its subdomains, such as host (or computer) names, static IP addresses, aliases, and mail exchangers.

Step 2: Configure BIND

BIND is the name of the program that implements DNS. It is also called the *name daemon*, or *named*, when the program is running. To set up and configure BIND, you need to modify the configuration file and the zone file.

The configuration file is located in this directory:

/etc/named.conf

The zone file name is based on the IP address of the server and begins with "db." For example, the zone file db.192.168.12.1 is located in this directory:

/var/named/db.192.168.12.1

Step 3: Set up a Mail Exchange (MX) record (optional)

If you provide mail service over the Internet, you need to set up an MX record for your server. For more information about this, read the next section.

Step 4: Start DNS service

To start DNS service, click the Network tab in Server Admin, click DNS Service, and choose Start DNS. A globe appears on the DNS icon when the service is running, and the first menu item changes to Stop DNS.

DNS Service Strategies and Tips

Using DNS With Mail Service

If you plan to provide mail service on your network, you must set up DNS so that incoming mail is sent to the appropriate mail host on your network. When you set up mail service, you define a series of hosts, known as *mail exchangers* or *MX hosts*, with different priorities. The host with the highest priority gets the mail first. If it's not available, the host with the next highest priority gets the mail, and so on.

For example, let's say your mail server's host name is "reliable" in the "example.com" domain. Without an MX record, your users' mail addresses would include the name of your mail server computer, like this:

user-name@reliable.example.com

If you want to change your mail server or redirect mail, you have to notify potential senders of a new address for your users. Or, you can create an MX record for each domain that you want to be handled by your mail server, and direct the mail to the correct computer.

When you set up an MX record, you should include a list of all possible computers that can receive mail for a domain. That way, if your server is busy or down, mail is sent to another one on the list. Each computer on the list is assigned a priority number. The one with the lowest number is tried first. If that computer isn't available, the computer with the next lowest number is tried, and so on. When a computer is available, it holds the mail and sends it to the main mail server when the main server becomes available, and then the server delivers the mail. A sample list might look like this:

example.com

10 reliable.example.com
20 our-backup.example.com
30 last-resort.example.com

MX records are used for outgoing mail, too. When your mail server sends mail, it looks at the MX records to see whether the destination is local or somewhere else on the Internet. Then the same process happens, in reverse. If the main server at the destination is not available, your mail server tries every available computer on that destination's MX record list, until it finds one that will accept the mail.

If you don't enter the MX information into your DNS server correctly, mail won't work. For more information about MX records, see the resources listed at the end of this chapter.

Using DNS With Dynamically Assigned IP Addresses

Dynamic DNS is a mechanism that lets you modify the IP address/domain name list without directing the name server to reload the edited list. This means you can update the name server remotely and modify DNS data easily.

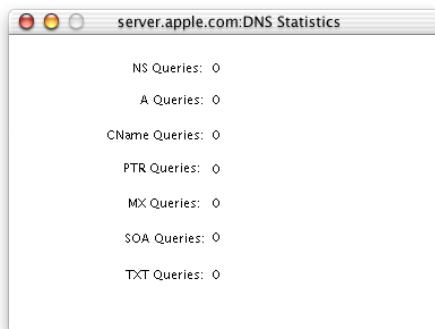
You can use dynamic DNS with DHCP service. DHCP assigns each client computer a dynamic IP address when the computer starts up. Because a DHCP server may assign IP addresses randomly, it can be useful to assign meaningful DNS names to these addresses on the fly. For instance, if “Bob” walks into work in the morning and starts up his computer, and the DHCP server assigns his computer a dynamic IP address, a DNS entry “bob.example.com” can be associated with that IP address. Even though Bob’s IP address may change every time he starts up his computer, his DNS name remains the same. This lets users communicate with Bob’s computer without knowing the IP address.

You can also use dynamic DNS to provide static host names for users who connect to the Internet through a modem. An ISP can set up dynamic DNS so a home computer has the same host name every time it connects.

Monitoring DNS Service

You can use Server Admin to check the status of DNS service, and to view some server query statistics.

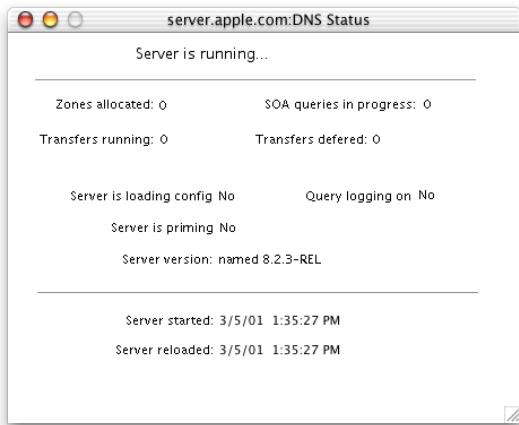
The DNS Statistics window shown here lists statistics for different types of queries. To view the DNS Statistics window, click the Network tab, then click DNS Service and choose DNS Statistics.



- *Name Server (NS)*: Asks for the authoritative name server for a given zone
- *Address (A)*: Asks for the IP address associated with a domain name
- *Canonical Name (CName)*: Asks for the “real name” of a server when given a “nickname” or alias. For example, mail.apple.com might have a canonical name of MailSrv473.apple.com
- *Pointer (PTR)*: Asks for the domain name of a given IP address (reverse lookup)

- *Mail Exchanger (MX)*: Asks which computer in a zone is used for email
- *Start Of Authority (SOA)*: Asks for name server information shared with other name servers, and possibly the email address of the technical contact for this name server
- *Text (TXT)*: Text records used by the administrator

To view the DNS Status window shown here, click the Network tab, then click DNS Service and choose DNS Status.

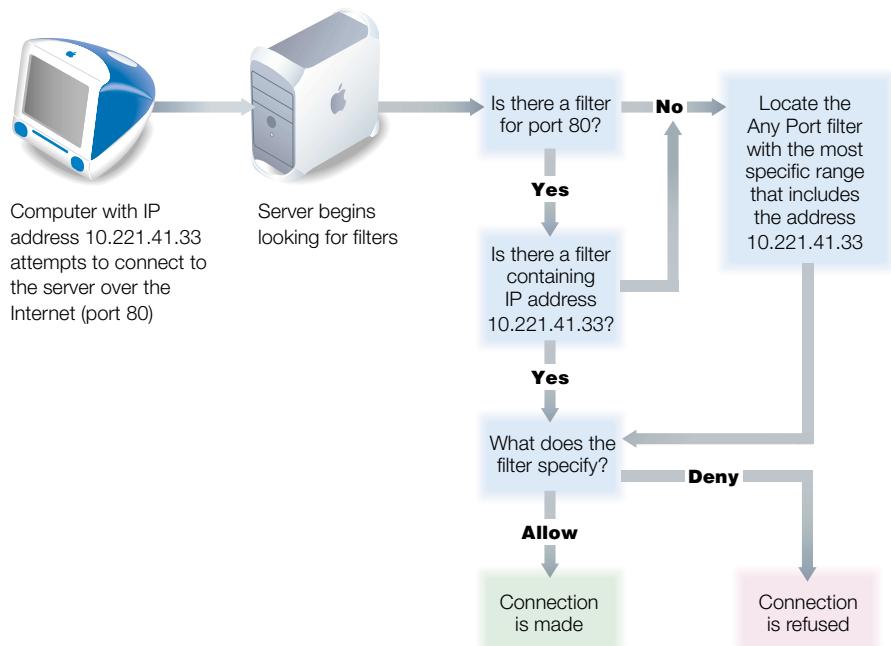


IP Filter Service

What Is IP Filter Service?

IP filter service is a software firewall that protects the network applications running on your Mac OS X Server. Turning on IP filter service is similar to erecting a wall to limit access. IP filter service scans incoming IP packets and rejects or accepts these packets based on the set of filters you create. You can restrict access to any IP service running on the server, and you can customize filters for all incoming clients, or a range of client IP addresses.

Services such as Web and FTP are identified on your server by a TCP or UDP port number. When a computer tries to connect to a service, IP filter service scans the filter list for a matching port number. If the port number is in the filter list, the filter applied is the one that contains the most specific address range. If the port number is not in the list, the Any Port filter that contains the most specific address range is used. The flow chart below illustrates this process.



The port filters you create are applied to TCP packets, and can also be applied to User Datagram Protocol (UDP) packets. In addition, you can set up filters for restricting Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), and NetInfo packets.

Important When you start IP filter service the first time, all incoming TCP packets are denied until you change the filters to allow access. By default, all addresses that are not specifically allowed are denied. Therefore, you must create filters if you want to allow access to your server. If you turn IP filter service off, all addresses are allowed access to your server.

Who Should Use IP Filter Service?

If you plan to share data over the Internet, and you do not have a dedicated router or firewall to protect your data from unauthorized access, you should use IP filter service. This service works well for a small to medium business, schools, and small or home offices.

Large organizations with a firewall can use IP filter service to exercise a finer degree of control over their servers. For example, individual workgroups within a large business, or schools within a school system, may want to use IP filter service to control access to their own servers.

Before You Set Up IP Filter Service

When you start IP filter service, the default configuration denies access to all incoming packets from remote computers. This provides the highest level of security. You can then add new IP filters to allow server access to those clients who require access to services.

First, think about the services that you want to provide on your server. Mail, Web, and FTP services generally require access from computers on the Internet. File and print services will most likely be restricted to your local subnet.

Once you decide which services you want to protect using IP filter service, you need to

- determine which IP addresses you want to allow access to your server
- determine which IP addresses you want to deny access to your server

Then, create the appropriate filters.

To learn how IP filters work and how to create them, read the sections that follow.

What Is a Filter?

A filter is made up of an IP address and a subnet mask, and sometimes a port number and access type. The IP address and the subnet mask together determine the range of IP addresses to which the filter applies.

IP address

IP addresses consist of four segments with values between 0 and 255, separated by dots (for example, 192.168.12.12). The segments in IP addresses go from general to specific (for example, the first segment might belong to all the computers in a whole company, whereas the last segment belongs to a specific computer on one floor of a building).

Subnet mask

The subnet mask, like the IP address, consists of up to four segments. You enter a mask to indicate which segments in the specified IP address can vary, and by how much. The only values you can use in a subnet mask segment are

- 0
- 128
- 192
- 224
- 240
- 248
- 252
- 254
- 255

The segments in a mask go from general to specific, so the earlier a zero appears in the segments of the subnet mask, the wider the resulting range of addresses. A subnet mask of 255.255.255.255 is the narrowest, and indicates a single IP address.

Any value except 255 in a segment of the subnet mask must be followed by zero segments. The following subnet mask examples are invalid because in each case, a value other than 255 is followed by a non-zero value:

- 255.255.128.255
- 255.0.128.128
- 255.255.252.255

Using Address Ranges

When you create filters using Server Admin, you enter an IP address and a subnet mask. Server Admin shows you the resulting address range, and you can change the range by modifying the subnet mask. When you indicate a range of possible values for any segment of an address, that segment is called a *wildcard*. The table below gives examples of address ranges created to achieve specific goals.

Goal	Sample IP address	Subnet mask	Address range
Create a filter that specifies a single IP address	10.221.41.33	255.255.255.255	10.221.41.33 (single address)
Create a filter that leaves the last segment of the IP address range as a wildcard	10.221.41.33	255.255.255.0	10.221.41.0 to 10.221.41.255
Create a filter that leaves part of the third segment and all of the fourth segment as a wildcard	10.221.41.33	255.255.252.0	10.221.40.0 to 10.221.43.255
Create a filter that applies to all incoming addresses		Select “All IP addresses”	All IP addresses

IP Address Precedence

If you create multiple filters for a port number, the filter that contains the most specific address range has precedence. The table below illustrates how this works. If a request comes in from an address that falls within the range specified on the first line, access is allowed. If it doesn't fall within that address range, the second line is checked. The last line, All, denies access. You cannot set both Deny and Allow for the exact same range of addresses.

Port	IP address	Mask	Access mode	Result
80 (Web)	10.221.41.33	255.255.255.255	Allow	Address 10.221.41.33 is allowed.
80 (Web)	10.221.41.33	255.255.252.0	Allow	Address in range 10.221.40.0 to 10.221.43.255 is allowed.
80 (Web)		All	Deny	All addresses are denied.

Multiple IP Addresses

A server can support multiple homed IP addresses, but IP filter service applies one set of filters to all server IP addresses. If you create multiple alias IP addresses, then the filters you create will apply to all of those IP addresses.

Setting Up IP Filter Service for the First Time

Once you've decided which filters you need to create, follow these steps to set up IP filter service. If you need more help to perform any of these steps, see IP Filter Help.

Step 1: Configure IP filter service

To configure IP filter service, click the Network tab in Server Admin. Then click IP Filter and choose Configure IP Filter Service. You can configure IP filter service to log denied and allowed packets, start up automatically, specify how rejections are handled, apply TCP port filters to UDP and other packets, and set up access for NetInfo.

For more information about the settings, see "IP Filter Service Settings" on page 290.

Step 2: Add filters to the IP filter list

Read "Before You Set Up IP Filter Service" on page 286 to learn how IP filters work and how to create them.

To add filters, click IP Filter and choose Show IP Filter List. Then click New and create a filter. For more information about creating a new filter, see "IP Filter Window Settings" on page 295.



Step 3: Start IP filter service

Click IP Filter and choose Start IP Filter Service.

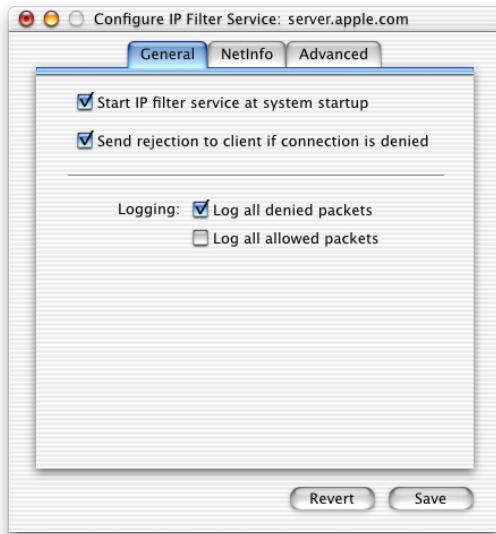
Important If you add or change a filter after starting IP filter service, the new filter will affect connections already established with the server. For example, if you deny all access to your FTP server after starting IP filter service, computers already connected to your FTP server will be disconnected.

IP Filter Service Settings

You use the Configure IP Filter Service window to make general settings, set up how filters are applied to NetInfo and UDP, and set up logging. To access the IP filter service settings, click the Network tab in Server Admin. Then click IP Filter and choose Configure IP Filter Service. The Configure IP Filter Service window has three tabs: General, NetInfo, and Advanced. Settings in each pane are described in the following sections.

General Settings

You use the General pane to set automatic startup, set up logging, and specify how rejections are handled. To access the General pane, click IP Filter and choose Configure IP Filter Service.



Start IP filter service at system startup

Select this option if you want IP filter service to start up automatically when the server starts up. Selecting this ensures that filtering is working in the event of power failures or accidental shutdowns.

Send rejection to client if connection is denied

Select this option to send a reply to clients whose connection attempts are denied.

Important Normally, you should choose this option since it prevents clients from flooding the server with retries. However, a malicious user could take advantage of the reply setting to launch a “denial-of-service attack” on your server by bombarding it with messages that are denied and then replied to. See “Preventing Denial-of-Service Attacks” on page 298.

Log all denied packets

Select this option to create a log entry for every connection attempt that is denied by one of the filters in your list.

Log all allowed packets

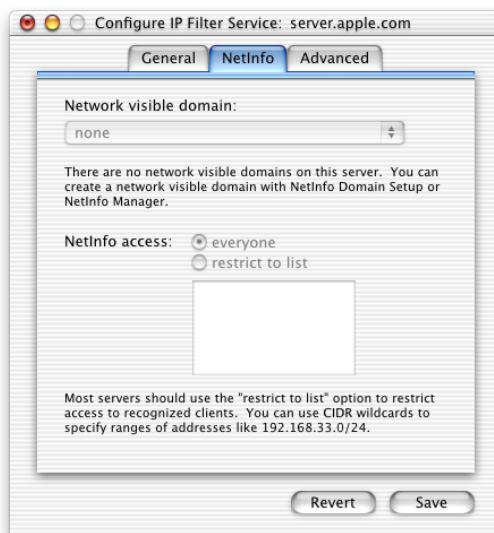
Select this option to create a log entry for every connection that is allowed by the filters in your list.

Important Both logging options can generate a lot of log entries, which fills up disk space and degrades the performance of the server. You should only use “Log all allowed packets” for limited periods of time.

NetInfo Settings

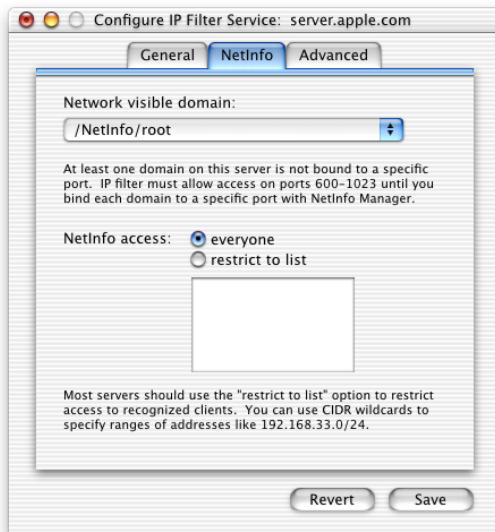
You use the NetInfo pane to allow or deny access to shared NetInfo domains. To access the NetInfo pane, click IP Filter and choose Configure IP Filter Service. Then click the NetInfo tab.

When the server has no shared NetInfos, the NetInfo pane is inactive.

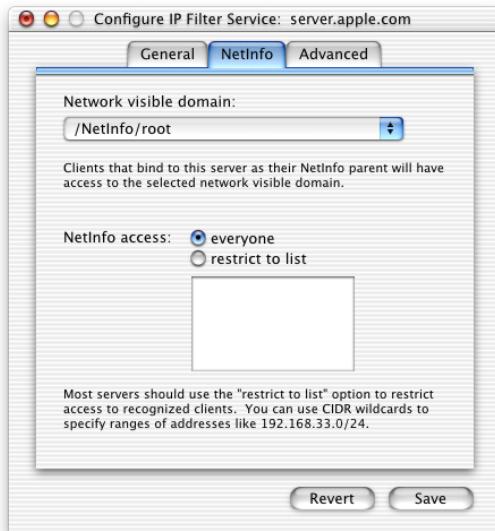


When the server has one or more shared NetInfo domains, choose a domain to work with from the “Network visible domain” pop-up menu.

If the domain has not been configured to use a specific port, NetInfo dynamically selects a port from the range 600 through 1023. You specify which IP addresses should be allowed access to any of those ports.



If the domain has been configured to use a specific port, you can specify IP addresses allowed to use that port. Onscreen help describes how to configure a shared NetInfo domain to use a specific port.



everyone

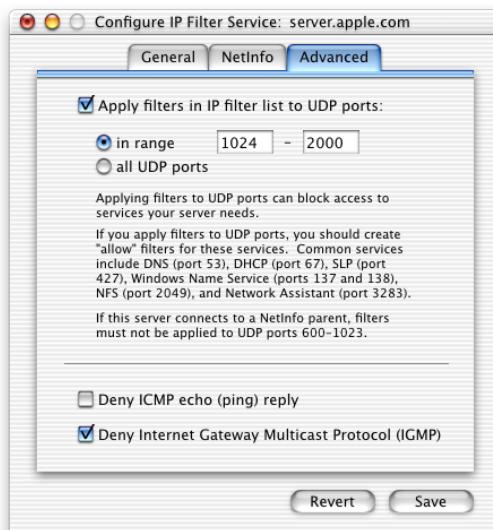
Select this option to allow all IP addresses to access the selected shared NetInfo domain. You should select this only if you have a firewall that protects your internal network from the Internet and blocks external traffic targeted at the ports used for NetInfo (111 and 600–1023 or a specific port configured for the domain). If you don't have a separate firewall, selecting this setting could compromise your server's security.

restrict to list

Select this option to specify the IP addresses that have NetInfo access. Enter an IP address in the text field and press Return before entering another. To enter a range of IP addresses, type a slash (/) after the IP address. For example, 192.168.33.3/24 means the range 192.168.33.0 to 192.168.33.255.

Advanced Settings

You use the Advanced pane to restrict UDP ports using the same list of filters that applies to TCP ports. To access the Advanced pane, click IP Filter and choose Configure IP Filter Service. Then click the Advanced tab.



Apply filters in IP filter list to UDP ports

To apply the filters to UDP ports, select this option and specify a range of UDP ports or select “all UDP ports.” By default, all UDP messages are allowed. Apply filters to UDP ports sparingly. Many services may use UDP to communicate with the server, and “deny” filters could create logjams in server traffic. Check the list of UDP ports in “Ports Used by Mac OS X Computers” on page 301 before you make any settings here.

You should also create “allow” filters for specific services to keep them from being blocked. These services include

- DNS on port 53
- DHCP on port 67
- SLP on port 427
- Windows Name Service browsing on ports 137 and 138
- Network Assistant on port 3283
- NFS on port 2049

UDP ports above 1023 are allocated dynamically by certain services, so their exact port numbers may not be determined in advance. For more information, see “Ports Used by Mac OS X Computers” on page 301.

Deny ICMP echo (ping) reply

Select this option if you don’t want to respond to pings from other host servers. Ping is a common network management tool based on the Internet Control Message Protocol (ICMP). Ping can determine the availability of a network server by sending a series of packets on a round-trip between two hosts, measuring average round-trip times and computing loss percentages. Not responding to network pings can help prevent a denial-of-service attack. However, other services that rely on being able to ping your server will be unable to detect its presence.

Deny Internet Gateway Multicast Protocol (IGMP)

Select this option if you don’t want to support multicast networking. IGMP is used by some hosts and routers to send packets to lists of hosts. QuickTime Streaming Server uses multicast addressing, as does Service Location Protocol (SLP). Turning off IGMP prevents these types of services from running correctly.

IP Filter Window Settings

You manage your IP filters using the IP filter list. To open the window for an IP filter, click one of the buttons at the bottom of the IP Filter List window. If you select an existing filter and click the Edit or Duplicate button, the resulting window has the current information for the selected filter. For information about working with the IP filter list, see “Working With the IP Filter List” on page 299.



Click the New button to create a new IP filter.



Access

Choose whether this filter will allow or deny server access for the IP addresses you specify.

Port Number

Choose a port number from the pop-up menu. If you want to create a filter that applies to all ports on the server, choose Any Port. If you don't see the port you want to use in the menu, type the port number in the text field. You can find a list of TCP and UDP port numbers in "Ports Used by Mac OS X Computers" on page 301.

Port Name

If you entered a non-standard port number, type a name to help you remember how this port is used.

Apply to

Select the IP addresses to which this filter will apply. Your choices are

- all IP addresses
- a range of IP addresses
- a single IP address

IP Address

Enter the IP address to which you want this filter to apply. If you chose "all IP addresses," this field is not available.

Find IP Address

Click this button if you don't know the IP address you want to filter. Enter the DNS host name to find its IP address. Click Apply to enter the found IP address in the IP Address field in the IP Filter window.

Subnet Mask

Enter the subnet mask you want to apply if you selected "a range of IP addresses." You can see the resulting address range below this field. For more information on using subnet masks, see "Using Address Ranges" on page 288.

Use My Subnet

Click this button to use the subnet mask value stored in the server's Network preferences.

IP Filter Service Strategies and Tips

The IP filters you create work together to provide security for your network. The examples that follow show you how to use filters to achieve some specific goals.

Block access to Internet users

To allow users on your subnet access to your server's Web service, but deny access to the general public on the Internet:

Access	Port	IP address
Allow	80 (Web)	In Server Admin, select "a range of IP addresses" and click Use My Subnet in the IP filter window.
Deny	80 (Web)	All

Block junk mail

To reject email from a junk mail sender with an IP address of 17.128.100.0 and accept all other Internet email:

Access	Port	IP address
Deny	25 (SMTP)	17.128.100.0
Allow	25 (SMTP)	All

Important Set up very specific address ranges in filters you create to block incoming SMTP mail. For example, if you set a filter on port 25 to deny mail from all addresses, you will prevent any mail from being delivered to your users.

Allow a customer to access the Apple file server

To allow a customer with an IP address of 10.221.41.33 to access an Apple file server:

Access	Port	IP address
Allow	548 (AFP/TCP)	10.221.41.33
Deny	548 (AFP/TCP)	All

Using Logs to Monitor IP Filter Service

When you configure IP filter service, you can choose to log denied and allowed packets. The Log Viewer in Server Admin provides access to all of Mac OS X Server's service logs. Click Log Viewer and choose System Software, then choose System Log and look for entries that begin with "ipfw."

The filters you create in Server Admin correspond to one or more rules in the underlying filtering software. Log entries show you the rule applied, the IP address of the client and server, and other information. For more information about rules and what they mean, see “Creating IP Filter Rules Using ipfw” on page 306.

Here are some examples of IP filter log entries and how to read them.

Log Example 1

```
Dec 12 13:08:16 ballch5 mach_kernel: ipfw: 65000 Unreach TCP  
          10.221.41.33:2190 192.168.12.12:80 in via en0
```

This entry shows that IP filter service used rule 65000 to deny (unreach) the remote client at 10.221.41.33:2190 from accessing server 192.168.12.12 on Web port 80 via Ethernet port 0.

Log Example 2

```
Dec 12 13:20:15 mayalu6 mach_kernel: ipfw: 100 Accept TCP  
          10.221.41.33:721 192.168.12.12:515 in via en0
```

This entry shows that IP filter service used rule 100 to allow the remote client at 10.221.41.33:721 to access the server 192.168.12.12 on the LPR printing port 515 via Ethernet port 0.

Log Example 3

```
Dec 12 13:33:15 smithy2 mach_kernel: ipfw: 10 Accept TCP  
          192.168.12.12:49152 192.168.12.12:660 out via lo0
```

This entry shows that IP filter service used rule 10 to send a packet to itself on port 660 via the loopback device 0.

Preventing Denial-of-Service Attacks

When the server receives a TCP connection request from a client to whom access is denied, by default it sends a reply rejecting the connection. This stops the denied client from resending over and over again. However, a malicious user could generate a series of TCP connection requests from a denied client IP address and force the server to reply continuously, locking out others who are trying to connect to the server. This is one type of *denial-of-service* attack.

To help prevent these attacks, do not select the “Send rejection to client if connection is denied” option in the General pane of the Configure IP Filter Service window. Be aware that turning off this option may cause certain clients to retry connections, which can result in server congestion. Select this option only if you think your server is vulnerable to this sort of attack.

Changing the Default IP Filter State

The Any Port filter All is the default filter for IP filter service. All incoming packets that are not contained in an address range for a listed port, or contained in an address range of the Any Port filter, will be either allowed or denied, depending on the access set for All.

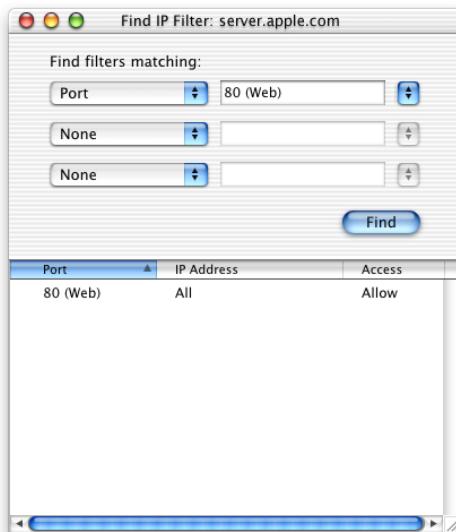
When you first start IP filter service, the Any Port filter All denies access by default, preventing you from granting access to your services that you didn't intend to allow. If you need to change the All filter to allow access, you can. However, you should not take this action lightly. Changing the default to allow means you must explicitly deny access to your services by setting up specific port filters for all the services that need protection.

Working With the IP Filter List

The IP filter list displays all the filters for the server. The filters are grouped by port number, which are listed in numeric order. Filters for a port are shown in the order of precedence, from filters with the most specific IP address range (or a single address) to filters with the widest address range (or All).

After you select a filter, you can click the Duplicate or Edit button to open the IP Filter window, described on page 295.

The Find button is a powerful tool that can help you find problems with your filters and check for security holes. When you click the Find button, you see the Find IP Filter window.



Choose the search criteria you want to use from the pop-up menus. You can search by port, IP address, and type of access (allow or deny). The results of your search are shown in the bottom section of the window.

Solving Problems With IP Filter Service

If you can't access the server over TCP/IP:

- Check the filters in the filter list. If you started IP filter service but have not added any additional filters, all TCP access to your server is denied by default.
- Stop IP filter service. Add new filters to your filter list that allow access to computers that have the IP addresses you specify. Then start IP filter service.

If you're having trouble locating specific filters:

- Use the Find button in the IP Filter List window to locate specific filters by IP address, port, or access type.

If you want to view denied packets:

- Turn on logging of denied packets in the Configure IP Filter Service window. To view logged entries, click the General tab in Server Admin and click Log Viewer. Choose System Software, then choose System Log from the pop-up menu.

Where to Find More Information About Network Services

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

For details about the following, see the RFC document indicated:

- *DCHP*: RFC 2131
- *Dynamic DNS*: RFC 2136 and RFC 2137
- *SLP DA*: RFC 2608
- *IP filter service*: See RFC 792 for information on ICMP. IGMP is documented in Appendix I of RFC 1112. Important multicast addresses are documented in the most recent Assigned Numbers RFC, currently RFC 1700.

For more information on DNS and BIND, see the following:

- *DNS and BIND*, 3rd edition, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 1998).
- The International Software Consortium Web site (www.isc.org).



Advanced Topics

This appendix contains information that experienced system or network administrators will find useful:

- “TCP/IP Topics,” below, includes a variety of topics, such as lists of TCP and UDP ports used by Mac OS X computers and instructions for setting up a private TCP/IP network.
- “File Format for Importing or Exporting Users and Groups” on page 308 provides an example of the XML statements used to describe users and groups in a file.
- “LDAP Data Specifications” on page 314 describes the proper format of data retrieved from LDAP servers and provides step-by-step instructions for setting up LDAP server access.
- “Backing Up Server Information” on page 328 provides instructions for backing up NetInfo and service-specific data on your server.

TCP/IP Topics

Read this section for information that will help you do advanced TCP/IP configuration.

Ports Used by Mac OS X Computers

The following tables show the TCP and UDP port numbers commonly used by Mac OS X computers and Mac OS X Servers. These ports can be used when you are setting up your IP filters.

Note: See www.faqs.org/rfcs to view the RFCs referenced in the tables.

TCP port	Used for	Reference
7	echo	RFC 792
20	FTP data	RFC 959
21	FTP control	RFC 959
22	ssh (secure shell)	

TCP port	Used for	Reference
23	Telnet	RFC 854
25	SMTP (email)	RFC 821
53	DNS	RFC 1034
79	Finger	RFC 1288
80	HTTP (Web)	RFC 2068
88	Kerberos	RFC 1510
110	POP3 (email)	RFC 1081
111	Remote Procedure Call (RPC)	RFC 1057
113	AUTH	RFC 931
115	sftp	
119	NNTP (news)	RFC 977
139	Windows file and print (SMB)	RFC 100
143	IMAP (email access)	RFC 2060
389	LDAP (directory)	RFC 2251
427	SLP (service location)	
443	SSL (HTTPS)	
514	shell	
515	LPR (printing)	RFC 1179
532	netnews	
548	AFP (AppleShare)	
554	Real-Time Streaming Protocol (QTSS)	RFC 2326
600–1023	Mac OS X RPC-based services (for example, NetInfo)	
626	IMAP Administration (Mac OS X mail service and AppleShare IP 6.x mail)	
660	Server Admin	

TCP port	Used for	Reference
985	NetInfo (when a shared domain is created using NetInfo Domain Setup)	
7070	Real-Time Streaming Protocol (QTSS)	
8000–8999	Web service	
16080	Web service with performance cache	
2236	Macintosh Manager	
24000–24999	Web service with performance cache	

UDP port	Used for	Reference
7	echo	
53	DNS	
67	DHCP server (BootP)	
68	DHCP client	
69	Trivial File Transfer Protocol (TFTP)	
111	Remote Procedure Call (RPC)	
123	Network Time Protocol	
137	Windows Name Service (WINS)	
138	Windows Datagram Service	
161	Simple Network Management Protocol (SNMP)	
427	SLP (service location)	
497	Retrospect	
513	who	
514	Syslog	
554	Real-Time Streaming Protocol (QTSS)	
600–1023	Mac OS X RPC-based services (for example, NetInfo)	

UDP port	Used for	Reference
985	NetInfo (when a shared domain is created using NetInfo Domain Setup)	
2049	Network File System (NFS)	
3283	Apple Network Assistant	
6970 and up	QTSS	
7070	Real-Time Streaming Protocol alternate (QTSS)	

Setting Up a Private TCP/IP Network

If you have a local area network that has a connection to the Internet, you must set up your server and client computers with IP addresses and other information that's unique to the Internet. You obtain IP addresses from your Internet service provider (ISP).

If it is likely that your local area network will never be connected to the Internet and you want to use TCP/IP as the protocol for transmitting information on your network, it's possible to set up a "private" TCP/IP network. When you set up a private network, you choose IP addresses from the blocks of IP addresses that the IANA (Internet Assigned Numbers Authority) has reserved for private intranets:

- 10.0.0.0–10.255.255.255 (10/8 prefix)
- 172.16.0.0–172.31.255.255 (172.16/12 prefix)
- 192.168.0.0–192.168.255.255 (192.168/16 prefix)

Important If you think you might want to connect to the Internet in the future, you should register with an Internet registry and use the IP addresses provided by the registry when setting up your private network. Otherwise, you'll need to reconfigure every computer on your network.

If you set up a private TCP/IP network, you can also provide DNS service. By setting up TCP/IP and DNS on your local area network, your users will be able to easily access file, Web, mail, and other services on your network.

Setting Up Multiple IP Addresses for a Port

When you first set up your server, the Setup Assistant lets you configure one IP address for each Ethernet port available on the server.

On some occasions, you may want to configure multiple IP addresses for a particular port. For example, if you use the server to host multiple Web sites, you may want to accept requests for different domain names (URLs) over the same port. To do so, you need to set up the port to have multiple configurations, one for each domain name, then use the Web module of Server Admin to map each site to a particular configuration.

To set up multiple IP addresses for a port:

- 1 Open System Preferences and click Network.
- 2 Choose Advanced from the Configure pop-up menu.
- 3 Click New.
- 4 Enter a name for the new port configuration and choose the port you are configuring from the Port pop-up menu. Click OK.
- 5 Choose the port configuration you just added from the Configure pop-up menu.
- 6 Click the TCP tab, then choose Manually from the Configure pop-up menu. Enter the new IP address and other information describing the port. Click Save.

Creating IP Filter Rules Using ipfw

You can use the ipfw command in conjunction with the IP Filter module of Server Admin when you want to

- Display rules created by the IP Filter module. Each filter translates into one or more rules.
- Create filters with characteristics that cannot be defined using the IP Filter module. For example, you may want to use rules specific to a particular kind of IP protocol. Or you may want to filter or block outgoing packets.
- Count the number of times rules are applied.

If you use ipfw, make sure you do not modify rules created using the IP Filter module. Changes you make to IP Filter module rules are not permanent. IP filter service re-creates any rules defined using the IP Filter module whenever the service is restarted. Here is a summary of how the IP Filter module assigns rule numbers:

Rule number	Used by IP Filter module for
10	Loop back
20	Discarding any packet from or to 127.0.0.0/8 (broadcast)
30	Discarding any packet from 224.0.0.0/3 (broadcast)
40	Discarding TCP packets to 224.0.0.0/3 (broadcast)
100–64000	User-defined port-specific filters
63200	Denying access for icmp echo reply. Created when “Deny ICMP echo reply” is selected in the Advanced pane of the Configure IP Filter Service window.
63300	Denying access for igmp. Created when Deny IGMP is selected in the Advanced pane of the Configure IP Filter Service window.
63400	Allowing any TCP or UDP packet to access port 111 (needed by NetInfo). Created when a shared NetInfo domain is found on the server.
63500	Allowing user-specified TCP and UDP packets to access ports needed for NetInfo shared domains. You can configure NetInfo to use a static port or to dynamically select a port from 600 through 1023. Then use the Configure IP Filter Service window to allow all or specific clients to access those ports.
64000–65000	User-defined filters for Any Port

To review the rules currently defined for your server, use the Terminal application to submit the ipfw show command. The show command displays four columns of information:

Column	Information
1	The rule number. The lower the number, the higher the priority of the rule.
2	The number of times the filter has been applied since it was defined
3	The number of bytes to which the filter has been applied
4	A description of the rule

```
ipfw show
```

```
0010    260      32688  allow log ip from any to any via lo*
0020    0         0      deny log ip from 127.0.0.0/8 to any in
0020    0         0      deny log ip from any to 127.0.0.0/8 in
0030    0         0      deny log ip from 224.0.0.0/3 to any in
0040    0         0      deny log tcp from any to 224.0.0.0/3 in
00100   1         52     allow log tcp from 111.222.33.3
                           to 111.222.31.3 660 in
...

```

To create new rules, use the ipfw add command. The following example defines rule 200, a filter that prevents TCP packets from a client with IP address 10.123.123.123 from accessing port 80 of the system with IP address 17.123.123.123:

```
ipfw add 200 deny tcp from 10.123.123.123 to 17.123.123.123 80
```

To delete a rule, use the ipfw delete command. This example deletes rule 200:

```
ipfw delete 200
```

For more information, consult the man pages for ipfw.

Where to Find More Information About Setting Up TCP/IP

For a tutorial on TCP/IP protocols, see this book:

- *TCP/IP Illustrated, Volume 1: The Protocols*, by W. Richard Stevens (Addison-Wesley Professional Computing Series, 1994).

This book has tips and guidelines for TCP/IP administration:

- *TCP/IP Network Administration*, 2d edition, by Craig Hunt (O'Reilly and Associates, 1997).

For information about setting up a private network, see information for RFC 1918 at this Web site:

www.faqs.org/rfcs

File Format for Importing or Exporting Users and Groups

The Users & Groups module of Server Admin lets you export users and groups in a NetInfo domain to a file, then use the file to import the definitions into a NetInfo domain on another server. The format used to encode user and group information is XML.

You can also create files containing user and group XML definitions by hand, using a text-editing application.

Note: Home directory information is not exported and cannot be encoded by hand in an XML file. Home directories are set up when you import users, as specified by the default home directory settings. Use the Users & Groups module in Server Admin on a server to set up the default home directory strategy before importing users into NetInfo domains on the server.

This section shows an example of a users and groups file, then describes how to encode your own file.

Example XML File

The example file contains three kinds of information:

- *Header information*: The header defines the elements (uglist, user, group, and so forth) that are in the body of the file. User information in the body of the file must precede group information. The header extends from the line labeled 1 through the line labeled 2 in the example.
- *User information*: The sample file contains attributes describing two users, Bob Smith and Jane Doe. Bob's definition extends from 4 through 40, and Jane's extends from 41 through 42.
- *Group information*: The sample file contains information for a group named *Imported Group* and a group named *Primary*, which have members Bob Smith and Jane Doe. The first group's definition extends from 43 through 48. The second one starts on 49 and finishes on 50.

```

<!XML version="1.0" > ---1
<!DOCTYPE MacOSXServer100 [
    <!ELEMENT uglist ( user | group* ) >
    <!ELEMENT user ( nameList? pass? homeDir? pluginDataList ) >
        <!Imported Group user
            comment CDATA #IMPLIED
            uid CDATA #IMPLIED
            gid CDATA #IMPLIED
            shell CDATA #IMPLIED
            logEnabled ( canLogin | noLogin ) "canLogin"
            isAdminUser ( isAdmin | notAdmin ) "notAdmin"
        >
        <!ELEMENT nameList name* >
        <!ELEMENT name EMPTY >
            <!Imported Group name
                text CDATA
            >
        <!ELEMENT pass EMPTY
            <!Imported Group pass
                format ( crypt| clearText | secure) "clearText"
                text CDATA
            >
        <!ELEMENT pluginDataList pluginData* >
        <!ELEMENT pluginData EMPTY >
            <!Imported Group pluginData
                signature CDATA #REQUIRED
                data CDATA #REQUIRED
            >
        <!ELEMENT group memberName* >
        <!Imported Group group
            name CDATA #REQUIRED
            gid CDATA #IMPLIED
        >
        <!ELEMENT memberName EMPTY >
            <!Imported Group memberName
                name CDATA #REQUIRED
            >
    >
] > ---2

```

```

<uglist>                                <--3
  <user>                                 <--4
    logEnabled = "canLogin"                <--5
    isAdminUser = "notAdmin"              <--6
    uid = "1200"                         <--7
    gid = "0"                            <--8
    shell = "/bin/tcsh">                  <--9
  < namelist >                         <--10
    < name >
      text = "bsmith" />                 <--11
    < name >
      text = "Bob Smith" />
  < /namelist >                        <--12
  < pass >
    format = "clearText"                 <--14
    text = "password" />                 <--15
<pluginDataList>                      <--16
  <pluginData>
    signature = "Mail"
    data = "<dict>
      <key>kAttributeVersion</key>        <--18
      <string>AppleMail 1.0</string>       <--19
      <key>kMailAccountState</key>         <--20
      <string>Enabled</string>             <--21
      <key>kIMAPLoginState</key>          <--22
      <string>IMAPAllowed</string>         <--23
      <key>kPOP3LoginState</key>          <--24
      <string>POP3Allowed</string>         <--25
      <key>kMailAccountLocation</key>       <--26
      <string>domain.example.com</string>   <--27
      <key>kAutoForwardValue</key>         <--28
      <string>user@example.com</string>     <--29
      <key>kNotificationState</key>         <--30
      <string>NotificationStaticIP</string>   <--31
      <key>kNotificationStaticIPValue</key>  <--32
      <string>[1.2.3.4]</string>            <--33
      <key>kSeparateInboxState</key>        <--34
      <string>OneInbox</string>             <--35

```

```

        <key>kShowPOP3InboxInIMAP</key>           <--36
        <string>HidePOP3Inbox</string>             <--37

        </dict>">                                <--38
    </pluginDataList>                         <--39
</user>                                         <--40

<user                                         <--41
    loginEnabled = "canLogin"
    isAdminUser = "notAdmin"
    uid = "1201"
    gid = "10"
    shell = "None">
    <namelist>
        <name = "jdoe" />
        <text = "Jane Doe" />
    </namelist>
    <pass>
        format = "clearText"
        text = "password2" />
</user>                                         <--42

<group                                         <--43
    name = "Imported Group"                   <--44
    gid = "2000" >
    <memberName>
        name = "bsmith" />                  <--45
    <memberName>
        name = "jdoe" />                  <--46
    </group>                                         <--47

<group                                         <--49
    name = "Primary"
    gid = "10" >
    <memberName>
        name = "bsmith" />
    <memberName>
        name = "jdoe" />
    </group>                                         <--50

</uglist>                                         <--51

```

Creating Your Own Users and Groups File

Follow these steps to enter information into a text file that you can import using the Users & Groups module of Server Admin:

- 1 Open a text-editing application.
- 2 At the beginning of the file, enter the header information exactly as shown in lines 1 through 2 in the example.
- 3 Enter the information exactly as shown in line 3. This line signals the start of your user and group information.
- 4 Enter the information exactly as shown in line 4. This line signals the start of your first user definition.
- 5 Enter the attribute describing whether the user can log in to the server. See line 5 for the format to use. Between the quotation marks, specify “canLogin” to enable login or “noLogin” to disable login.
- 6 Enter the attribute describing whether the user can act as server administrator. See line 6 for the format to use. Between the quotation marks, specify “isAdmin” to enable administrator privileges or “notAdmin” to disable them for the user.
- 7 Enter the user ID as shown in line 7. Between the quotation marks, specify a number uniquely identifying the user.
- 8 Enter the user’s primary group ID as shown in line 8, specifying a number for a group defined later in the file (steps 14 through 20) between the quotation marks.
- 9 Identify the default shell to use for command-line interactions with the server. See line 9 for the format to use. Between the quotation marks, enter the path and filename of the script or enter “None” to prevent command-line access.
- 10 Enter the user’s name and short name as shown in lines 10 through 12. Enter all information exactly as shown except the information between the quotation marks, which are the names you assign.
- 11 Enter the user’s password as shown in lines 13 through 15. Specify the information on lines 13 and 14 exactly as shown. On the next line, specify the user’s password string within quotation marks, as shown in line 15.
- 12 If the user will not be using mail service on a Mac OS X Server, skip this step. Otherwise, enter the user’s mail attributes like this:
 - a Enter lines 16 through 19 exactly as shown.
 - b Enter two lines defining how the user’s mail is handled (the mail state). Identify the attribute exactly as shown in line 20. Specify a value for the attribute as line 21 illustrates. Use a value of “Off” to disable mail delivery, “Enabled” to enable it, or “Forward” to forward the user’s mail.

- c** Enter two lines defining the user's IMAP login state attribute, which describes whether the user can access mail using the Internet Message Access Protocol. Identify the attribute exactly as shown in line 22. Specify a value for the attribute as line 23 illustrates. Use a value of "IMAPAllowed" to let the user access mail using IMAP or "IMAPDeny" to prevent IMAP access.
 - d** Enter two lines defining the user's POP3 login state attribute, which describes whether the user can access mail using the Post Office Protocol. Identify the attribute exactly as shown in line 24. Specify a value for the attribute as line 25 illustrates. Use a value of "POP3Allowed" to let the user access mail using POP3 or "POP3Deny" to prevent POP3 access.
 - e** Enter two lines defining the user's mail account location attribute, which describes where the user's mail is stored. Identify the attribute exactly as shown in line 26. Specify a value for the attribute as shown in line 27. The value should be the domain name or IP address of the server that stores the user's mail.
 - f** If you assigned the user's mail account state the value "Forward," enter two lines defining the user's autoforward attribute. Identify the attribute exactly as shown in line 28. Specify a value for the attribute as shown in line 29. Use a value that is a valid RFC 822 email address.
 - g** Enter two lines defining the user's notification state attribute, which determines whether the user is automatically notified when new mail has arrived. Identify the attribute exactly as shown in line 30. Specify a value for the attribute as line 31 illustrates. Use a value of "NotificationOff" to avoid automatic notification, "NotificationLastIP" to send a notification to the last address from which the user logged in, or "NotificationStaticIP" to send a notification to a specific IP address.
 - h** If you assigned the user's notification state attribute the value "NotificationStaticIP," enter two lines defining the notification static IP address attribute. Identify the attribute exactly as shown in line 32. Specify the IP address as line 33 illustrates.
 - i** Enter two lines defining the user's separate inbox state attribute, which determines whether the user manages POP3 and IMAP mail using different inboxes. Identify the attribute exactly as shown in line 34. Specify a value for the attribute as line 35 illustrates. Use a value of "DualInbox" to enable using different inboxes. Otherwise, use a value of "OneInbox."
 - j** Enter two lines defining the user's show POP3 inbox in IMAP attribute, which determines whether an IMAP folder named "POP Inbox" is shown. Identify the attribute exactly as shown in line 36. Specify a value for the attribute as line 37 illustrates. Use a value of "ShowPOP3Inbox" to display the folder. Otherwise, use a value of "HidePOP3Inbox."
 - k** Complete the user's definition by entering lines 38 through 40 exactly as shown.
- 13** Repeat steps 4 through 12 for any additional users you want to add to the file.
- 14** Enter the information exactly as shown in line 43. This line signals the start of your first group definition.
- 15** Enter the group name between quotation marks as shown in line 44.

- 16** Enter the group ID between quotation marks as shown in line 45.
- 17** Enter the name of a user defined earlier in the file that you want to belong to the group. Enter the information in line 46 exactly as shown. On the next line, specify the user's short name as line 47 illustrates, enclosing it within quotation marks.
- 18** Repeat step 17 for each user you want to add to the group.
- 19** Terminate the group's definition by entering the information exactly as shown in line 48.
- 20** Repeat steps 14 through 19 for any additional groups you want to define in the file.
- 21** Enter line 51 exactly as shown at the end of your file. This line signals the end of your user and group information.
- 22** Save the file, using the extension "xml."
- 23** In Server Admin, use the Users & Groups module to import the user and group definitions in the file. Home directories are set up using the default home directory settings.

Where to Find More Information About XML

For information on creating and editing XML files, see these books:

- *The XML Pocket Reference*, by Robert Eckstein (O'Reilly, 1999).
- *Presenting XML*, by Richard Light (Sams.Net Publishing, 1997).
- *Learning XML*, by Erik Ray, with Christopher Maoen (O'Reilly, November 2000).
- *The XML Handbook*, by Charles F. Goforth (Prentice Hall PTR, 1998).

See this Web site for a comprehensive list of books about XML:

www.oasis-open.org/cover/bib-strt.html

LDAP Data Specifications

This section describes the data your server can retrieve from an LDAP server for use when

- authenticating and authorizing users
- finding network services, such as AFP servers and printers

It also describes the default LDAP data item names, which are used when you do not do any explicit mapping with the Directory Setup application.

Additionally, it describes how to use the Directory Setup application to configure a Mac OS X Server to use data on LDAP servers. Make sure that any LDAP server your Mac OS X Server accesses provides the needed data in the format described in this section.

Mapping User Data

The following table describes how your Mac OS X Server uses data about users. Determine which data items you want your server to retrieve from an LDAP server. Note that “All services” in the far-left column includes AFP, SMB, FTP, HTTP, NFS, WebDAV, POP, IMAP, Server Admin, the Mac OS X login window, and Macintosh Manager.

Server component	Data item used	Dependency
All services	RecordName	Required for authentication
All services	RealName	Required for authentication
All services	Password	Required for authentication If the LDAP server contains a crypt password, it is retrieved and used for authentication. Otherwise, the LDAP server validates the password using the LDAP BIND command.
All services	UniqueID	Required for authorization (for example, file permissions and mail accounts)
All services	PrimaryGroupID	Optional, but recommended. Used for authorization (for example, file permissions and mail accounts).
■ FTP service ■ Web service ■ Apple file service ■ NFS service ■ Macintosh Manager ■ Mac OS X login window ■ Application and system preferences	HomeDirectory	Optional
Mail service	MailAttribute	Required for login to mail service on your server
Mail service	EMailAddress	Optional

When you use Directory Setup to configure your server to access the LDAP server, use the Records pane to map the record type “Users” to one or more search bases on the LDAP server that provide the user data items you need. Then use the Data pane to map each item to one or more LDAP fields that can supply values for them. Ensure that each user data item your server will need is available on the LDAP server in the format described in the following table:

Data item	LDAP mapping format	Sample values
RecordName: a list of names associated with a user; for authentication, both RecordName and RealName should be present	ASCII	Dave David Mac DMacSmith
RealName: a single name, usually the user’s full name	ASCII	David L. MacSmith, Jr.
UniqueID: a unique user identifier	Unsigned 32-bit ASCII string of digits 0–9	Range is 100 to 4,294,967,295. Values below 100 are typically used for system accounts. Zero is reserved for use by the system.
Password: the user’s password	UNIX crypt	
PrimaryGroupID: a user’s primary group association	Unsigned 32-bit ASCII string of digits 0–9	Range is 0 to 4,294,967,295.
Comment: any documentation you like	ASCII	John is in charge of product marketing.
UserShell: the location of the default shell for command-line interactions with the server	Path name	/bin/tcsh /bin/sh None

Data item	LDAP mapping format	Sample values
MailAttribute: a user's mail service configuration. Refer to the next table for information on individual fields.	Mac OS X property list	<pre><dict> <key>kAttributeVersion</key> <string>Apple Mail 1.0</string> <key>kAutoForwardValue</key> <string>user@example.com</string> <key>kIMAPLoginState</key> <string>IMAPAllowed</string> <key>kMailAccountLocation</key> <string>domain.example.com</string> <key>kMailAccountState</key> <string>Enabled</string> <key>kNotificationState</key> <string>NotificationStaticIP</string> <key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string> <key>kPOP3LoginState</key> <string>POP3Allowed</string> <key>kSeparateInboxState</key> <string>OneInbox</string> <key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string> </dict></pre>
EMailAddress: an email address to which mail should be automatically forwarded when a user has no MailAttribute defined	Any legal RFC 822 email address or a valid "mailto:" URL	<pre>user@example.com mailto:user@example.com</pre>
HomeDirectory: the location of an AFP-based home directory	Mac OS X property list	<p><homeDir></p> <pre><url>afp://server/sharepoint</url> <path>usershomedirectory</path> </homeDir></pre> <p>In the following example, Tom King's home directory is K-M/Tom King, which resides beneath the share point directory, Users:</p> <pre><homeDir> <url>afp://example.com/Users</url> <path>K-M/Tom King</path> </homeDir></pre>

Ensure that each MailAttribute field you configure your server to retrieve from an LDAP server is in the format described in the following table. If any field contains an incorrect value, the MailAttribute is ignored (in other words, treated as if MailAccountState were “Off”).

MailAttribute field	LDAP mapping format	Sample values
AttributeVersion	A required case-insensitive value that must be set to “AppleMail 1.0”	<key>kAttributeVersion</key> <string>AppleMail 1.0</string>
MailAccountState	A required case-insensitive keyword describing the state of the user’s mail. It must be set to one of these values: “Off”, “Enabled”, or “Forward”.	<key>kMailAccountState</key> <string>Enabled</string>
POP3LoginState	A required case-insensitive keyword indicating whether the user is allowed to access mail via POP. It must be set to one of these values: “POP3Allowed” or “POP3Deny”.	<key>kPOP3LoginState</key> <string>POP3Deny</string>
IMAPLoginState	A required case-insensitive keyword indicating whether the user is allowed to access mail using IMAP. It must be set to one of these values: “IMAPAllowed” or “IMAPDeny”.	<key>kIMAPLoginState</key> <string>IMAPAllowed</string>
MailAccountLocation	A required value indicating the domain name or IP address of the Mac OS X Server responsible for storing the user’s mail	<key>kMailAccountLocation</key> <string>domain.example.com</string>

MailAttribute field	LDAP mapping format	Sample values
AutoForwardValue	A required field only if MailAccountState has the value “Forward”. The value must be a valid RFC 822 email address.	<key>kAutoForwardValue</key><string>user@example.com</string>
NotificationState	An optional keyword describing whether to notify the user whenever new mail arrives. If provided, it must be set to one of these values: “NotificationOff”, “NotificationLastIP”, or “NotificationStaticIP”. If this field is missing, “NotificationOff” is assumed.	<key>kNotificationState</key><string>NotificationOff</string>
NotificationStaticIPValue	An optional IP address, in bracketed, dotted decimal format ([xxx.xxx.xxx.xxx]). If this field is missing, NotificationState is interpreted as “NotificationLastIP”. The field is used only when NotificationState has the value “NotificationStaticIP”.	<key>kNotificationStaticIPValue</key><string>[1.2.3.4]</string>

MailAttribute field	LDAP mapping format	Sample values
SeparateInboxState	<p>An optional case-insensitive keyword indicating whether the user manages POP and IMAP mail using different inboxes. If provided, it must be set to one of these values: “OneInbox” or “DualInbox”.</p> <p>If this value is missing, the value “OneInbox” is assumed.</p>	<pre><key>kSeparateInboxState</key> <string>OneInbox</string></pre>
ShowPOP3InboxInIMAP	<p>An optional case-insensitive keyword indicating whether POP messages are displayed in the user’s IMAP folder list. If provided, it must be set to one of these values: “ShowPOP3Inbox” or “HidePOP3Inbox”.</p> <p>If this field is missing, the value ShowPOP3Inbox is assumed.</p>	<pre><key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string></pre>

Mapping Network Service Data

You can configure your server to access LDAP data describing network services, such as file servers and printers. Mac OS X applications that use NSL (Network Service Locator) to discover network services use the data to make these services available to users.

For example, if an LDAP server stores records describing Web servers you want to give users access to, these Web servers would be listed in the Finder when users choose the Connect to Server command.

To configure your server to access LDAP network service data, use the Records pane of Directory Setup to map record types for each service to one or more search bases on the LDAP server that provide the network data. Record types you might choose include AFPServer, WebServer, and Printers. Then, for each record type, use the Data pane to map the two data items described in the following table to one or more LDAP fields that can supply values for them:

Data item	LDAP mapping format	Sample values
RecordName: the name of a record	ASCII	Mrs. Jones' classroom
URLForNSL: the network location of the service	A valid URL	afp://afp.example.org/ https://securesite.example.org

Using the Default Mappings

If you are setting up an LDAP server for the first time, you can take advantage of default LDAP data item names. When LDAP field names match those shown in the following table, you do not need to map names using the Data pane in Directory Setup:

Data item	Default LDAP field name
RecordName	cn, sn, dn
EMailAddress	mail, email
UniqueID	unixid
RealName	realname
MailAttribute	applemail
Comment	comment
Group	grouplist
Password	passwd
PrimaryGroupID	groupid
HomeDirectory	home, homeloc
URLForNSL	networklocurl
GroupMembership	userlist
RecordAlias	aliasdata
UserShell	shell

Note that Group, optionally associated with a user record, lists the groups a user belongs to, whereas GroupMembership lists users belonging to a group.

Configuring LDAP Access

This section describes the steps for configuring LDAP access to all data for a user that can be retrieved from an LDAP server, as shown for the following example user:

Data item	Sample LDAP field name	Sample LDAP value
RecordName	shortname	bsmith
UniqueID	userid	1200
RealName	realname	Bob Smith
MailAttribute	applemail	<dict> <key>kAttributeVersion</key> <string>Apple Mail 1.0</string> <key>kAutoForwardValue</key> <string>user@example.com</string> <key>kIMAPLoginState</key> <string>IMAPAllowed</string> <key>kMailAccountLocation</key> <string>domain.example.com</string> <key>kMailAccountState</key> <string>Enabled</string> <key>kNotificationState</key> <string>NotificationStaticIP</string> <key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string> <key>kPOP3LoginState</key> <string>POP3Allowed</string> <key>kSeparateInboxState</key> <string>OneInbox</string> <key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string> </dict>
Comment	comment	Bob is a good resource for network administration.
Password	passwd	If the password attribute mapping is deleted or unmapped, the Mac OS X Server attempts to use the LDAP BIND command to authenticate users. Otherwise, the password field should contain a UNIX crypt password, which the server will use for authentication.

Data item	Sample LDAP field name	Sample LDAP value
PrimaryGroupID	primarygroupid	10
HomeDirectory	homedir	The user's home directory, R-S/Bob Smith, is located within a share point directory named Users: <homeDir> <url>afp://example.com/Users</url> <path>R-S/Bob Smith</path> </homeDir>
UserShell	loginshell	/bin/sh

The steps also describe how to configure LDAP access to information about a group:

Data item	Sample LDAP field name	Sample LDAP value
RecordName	gn	Primary
UniqueID	groupid	10
GroupMembership	groupmemberlist	bsmith, jdoe

You cannot use LDAP data to assign administrator rights to a user. If you want a user to be able to use server administration applications, add the user to the Administrator group in the server's local NetInfo domain using the Users & Groups module of Server Admin.

Here are the steps you must follow to configure a server to access user and group information:

- 1 Set up the LDAP server:
 - a Configure the LDAP server to support LDAP-based authentication and password checking.
 - b Modify LDAP server entries and attributes as necessary to provide the data needed by Mac OS X Server.
- 2 Enable LDAP support for the Mac OS X Server:
 - a Open the Directory Setup application, located in Applications/Utilities.
 - b Click the lock to log in as server administrator.
 - c Select LDAPv2, then click Configure.
 - d Click New.

- 3** Identify the LDAP server:
 - a** Click the Identity tab.
 - b** In the Name field, enter a descriptive name for the LDAP server.
 - c** In the Address field, enter the LDAP server's domain name or IP address.
- 4** Define the LDAP search base:
 - a** Click the Records tab.
 - b** Select Users in the Record Type list. Then edit the default "Maps to" value (ou=people, o=company name) to specify one or more search bases on the LDAP server that provide user information.
 - c** Select Groups in the Record Type list. Then edit the default "Maps to" value (ou=groups, o=company name) to specify one or more search bases on the LDAP server that provide group information.
- 5** Map user data:
 - a** Click the Data tab to map user information needed by Mac OS X Server to LDAP server fields that can provide the data. "Mapping User Data" on page 315 describes the format in which individual data item values must be returned from the LDAP server.
 - b** Map the names a user can be known by, including the user's short name. In the Data Type column, select RecordName. In the "Maps to" column, change the default LDAP field names (cn, sn, and dn) as required to identify one or more LDAP fields that store user names.
 - c** Map the user ID, a number that uniquely identifies a user. In the Data Type column, select UniqueID. Then change the default LDAP field name (unixid) if required to identify the LDAP field that stores the user ID.
 - d** Map the full user name. In the Data Type column, select RealName. Then change the default LDAP field name (realname) if required to identify the LDAP field that stores the full name.
 - e** If users will be using mail service on the server, map the mail attribute. In the Data Type column, select MailAttribute. Then change the default LDAP field name (applemail) if required to identify the LDAP field that stores the mail attribute in the required format.
For users without a mail attribute, map the forwarding address. In the Data Type column, select EMailAddress. Then change the default LDAP field names (mail and email) if required to identify the LDAP field that stores the forwarding address.
 - f** Map the user password only if the LDAP server stores user passwords in UNIX crypt format. Change the default LDAP field name (passwd) if required to identify the LDAP field that stores the password.
 - g** Map the primary group ID. In the Data Type column, select PrimaryGroupID. Then change the default LDAP field name (groupid) if required to identify the LDAP field that stores the group ID for the user's primary group.

- h** Map the home directory. In the Data Type column, select HomeDirectory. Then change the default LDAP field names (home and homeloc) if required to identify the LDAP field that stores the home directory information in the required format.
 - i** Map the user login shell, the default shell used for command-line interactions with the server. In the Data Type column, select UserShell. Then change the default LDAP field name (shell) if required to identify the LDAP field that stores the path and filename of the shell. Enter “None” if no command-line interactions should be permitted.

6 Map group data (if needed):

 - a** In the Data pane, map group information needed by Mac OS X Server to LDAP server fields that should be used to retrieve the data.
 - b** Map the group name. In the Data Type column, select RecordName. In the “Maps to” column, enter one or more LDAP fields that store group names.
 - c** Map the group ID, a number that uniquely identifies a group. In the Data Type column, select UniqueID. Then enter the LDAP field that stores the group ID.
 - d** Map the group members. In the Data Type column, select GroupMembership. Then change the default LDAP field name (userlist) if required to identify the LDAP field that stores a list of users associated with the group. Users should be identified using their short names.

7 Define the attributes of connections between Mac OS X Server and the LDAP server:

 - a** Click the Access tab.
 - b** Select “Use anonymous access” if the Mac OS X Server should connect with the LDAP server without using a name and password. Otherwise, select “Use the username and password below” and enter the distinguished name (for example, cn=admin, cn=users, dc=example, dc=com) and password that your server should use to establish an LDAP server connection. Ensure that the LDAP server is configured to accept any name and password you specify.
 - c** Enter the number of seconds for the open & close timeout, which defines the maximum time to maintain a connection. The default is 120 seconds.
 - d** Enter the number of seconds for the search timeout, which defines the maximum time to spend searching for data on the LDAP server. The default is 120 seconds.
 - e** Identify the port that should be used for the connection. The default is port 389. Ensure that any number you specify is actually used by the LDAP server.
 - f** Click OK.
 - g** Select the Enable checkbox to make the LDAP server you just configured available for use by directory services, then close the window and click Save.
 - h** In the Services pane, select the LDAPv2 checkbox, then click Apply if it is enabled.

- 8** Indicate how you want Mac OS X Server to use data stored on the LDAP server:
- a** If you always want your server to search records on the LDAP server when information for a user is not found in NetInfo domains the server is configured to use, add the LDAP server to the search policy.

Click the Authentication tab. Choose “NetInfo network” from the Search pop-up menu to display the default NetInfo hierarchy configured for the server. If the hierarchy includes one or more parent domains, make a note of them.

Choose “Custom path” from the Search pop-up menu. If the server’s default NetInfo hierarchy includes one or more parent domains, add each parent domain to the list. Click Add, select the parent for the local domain, then click Add; repeat this sequence for the next parent, if any, continuing until all the domains in the default NetInfo hierarchy are listed.

To add an LDAP server to the search policy, click Add, select the LDAP server, then click Add. If necessary, drag the LDAP Server entry so it appears below the default NetInfo hierarchy. The higher you place it in the list, the sooner it is searched when an entry above it in the list contains no information for a user. Click Apply.
 - b** If you want your server to search records on the LDAP server only when information for specific users is not found in any NetInfo domain, define an alias for each of these users. Open Server Admin, click the General tab, click Users & Groups, and choose Find Users & Groups. Choose “Selected directories” from the “Find in” pop-up menu to select the LDAP server. Set up search criteria for the user, then click Find. Choose Show Users & Groups List from the Users & Groups menu, and select the domain in which you want to add the alias. Drag the user from the Find Results window to the Users & Groups List window.

Backing Up Server Information

You should back up your server's system files regularly so data loss is minimized if there's a problem with the server and you need to restore the files.

At a minimum, back up files containing this information:

- *Root and administrator user IDs:* System files are owned by root or system administrator user IDs that exist at the time they are created. Should you need to restore system files, the same IDs should exist on the server so that the original permissions are preserved. To ensure that you can re-create these user IDs, periodically export the server's user and group information to a file using Server Admin's Users & Groups module.
- *NetInfo data:* Information associated with NetInfo domains is stored in files that reside in /var/db/netinfo/. Back up the entire directory.
When the Authentication Manager for Windows clients is enabled, a file containing the encrypted password for each NetInfo domain on the server is stored in /var/db/netinfo/. If the NetInfo database name is MyDomain, the encryption key file is .MyDomain.tim.
- *Mail database:* The mail service database resides in /Library/AppleMailServer/MacOSXMailDB. Back up this file.
- *Directory services configuration:* Configurations set up using the Directory Setup application are stored in /Library/Preferences/DirectoryService/. Back up the entire directory.

Mac OS X Server Information Worksheet

This appendix contains a worksheet for recording information about your server. It is the same as the worksheet provided in the fold-out card, *Getting Started With Mac OS X Server*, which came with your server installation CDs. You can print the worksheet in this appendix if you need extra copies of it.

Refer to *Getting Started With Mac OS X Server* for information about how to use this worksheet.

Mac OS X Server Information Worksheet

The Mac OS X Server Setup Assistant asks you for the information in this worksheet. If you don't have all of the networking and Ethernet port planning information, your network administrator or Internet service provider (ISP) can give it to you.

Important

This worksheet contains important security information. Keep it in a safe place.

Identification information	
Mac OS X Server serial number	Enter the number that is printed on your CD:

Security information	
Administrator (owner) name	Enter a name shorter than 100 characters (the name can include spaces):
Administrator short name	Enter a name with 8 or fewer characters and no special characters other than a period (.), hyphen (-), or underscore (_):
Administrator password	Make sure the Caps Lock key is not pressed when you enter the password. This password is also used for the root user until you change it:

Networking information	
NetInfo data sharing (Select one)	<input type="checkbox"/> The server will use the local NetInfo domain only. <input type="checkbox"/> The server will access a NetInfo domain on another server: Enter the static IP address of that server: Enter the filename (server tag) of the NetInfo domain. Specify "network" if the domain was set up using Setup Assistant: Note: Select the first option if you're not sure what to select. For information about NetInfo, see the administrator's guide and <i>Understanding and Using NetInfo</i> .
Server's host name	Enter a name that begins with a letter and contains only letters, numbers, or the underscore (_):
IP address(es) of domain name server (DNS)	
DNS Search domain(s)	If you wish, enter one or more domain names (for example, apple.com), separated by commas:
Server's AppleTalk name	Enter a name no longer than 31 characters:

continued

Mac OS X Server Information Worksheet *continued*

Your server has a built-in Ethernet port and may have additional ports installed on an Ethernet card. When you use the Setup Assistant, you'll specify how each port should be used (TCP/IP and/or AppleTalk) and enter address information for the ports. While AppleTalk is optional, it can be used on one port by Apple file service and print service.

If you don't select TCP/IP and/or AppleTalk for a port, the Setup Assistant won't configure that port. For each port you choose to configure, you'll see a panel where you enter the address information.

Tip

If you plan to use a multiport Ethernet card, consult with a networking professional.

You must configure one port using the Setup Assistant. You can use the Network pane of System Preferences to configure the remaining ports.

Ethernet port planning					
Use for TCP/IP and/or AppleTalk? (AppleTalk can be active on only one port)					
Built-in Ethernet port:	TCP/IP <input type="checkbox"/>	AppleTalk <input type="checkbox"/>	Ethernet card port 3:	TCP/IP <input type="checkbox"/>	AppleTalk <input type="checkbox"/>
Ethernet card port 1:	TCP/IP <input type="checkbox"/>	AppleTalk <input type="checkbox"/>	Ethernet card port 4:	TCP/IP <input type="checkbox"/>	AppleTalk <input type="checkbox"/>
Ethernet card port 2:	TCP/IP <input type="checkbox"/>	AppleTalk <input type="checkbox"/>			
Specify the following information using the IP address format (for example, 192.168.12.12):					
Built-in Ethernet port		Ethernet card port 3			
IP Address:	IP Address:		
Subnet Mask:	Subnet Mask:		
Router Address:	Router Address:		
Ethernet card port 1		Ethernet card port 4			
IP Address:	IP Address:		
Subnet Mask:	Subnet Mask:		
Router Address:	Router Address:		
Ethernet card port 2					
IP Address:				
Subnet Mask:				
Router Address:				

Glossary

A, B

AFP (Apple Filing Protocol) A client/server protocol used by Macintosh or Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

C

CGI (Common Gateway Interface) A script or program that adds dynamic functions to a Web site. A CGI sends information back and forth between a Web site and an application that provides a service for the site. For example, if a user fills out a form on the site, a CGI could send the message to an application that processes the data and sends a response back to the user.

D, E

DHCP (Dynamic Host Configuration Protocol) A protocol used to distribute IP addresses to client computers. Each time a client computer starts up, it looks for a DHCP server, then it requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a “lease period”—the length of time the client computer may use the address.

DNS (Domain Name System) A distributed database that maps IP addresses to domain names. A DNS server keeps a list of names and the IP addresses associated with each name. When a computer needs to find the IP address for a name, it sends a message to the DNS server (also known as a *name server*). The name server looks up the IP address and sends it back to the computer. If the name server doesn’t have the IP address locally, it sends messages to other name servers on the Internet until the IP address is found.

F, G

FTP (File Transfer Protocol) A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

H

HTML (Hypertext Markup Language) The set of symbols or codes inserted in a file to be displayed on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user.

HTTP (Hypertext Transfer Protocol) An application protocol that defines the set of rules for exchanging files on the World Wide Web.

I, J, K

IANA (Internet Assigned Numbers Authority) An organization responsible for allocating IP addresses, assigning protocol parameters, and managing domain names.

ICMP (Internet Control Message Protocol) A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use it to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

IGMP (Internet Group Management Protocol) An Internet protocol used by hosts and routers to send packets to lists of hosts that want to participate, which is known as *multicasting*. QuickTime Streaming Server uses multicast addressing, as does Service Location Protocol (SLP).

IMAP (Internet Message Access Protocol) A client-server mail protocol that allows users to access their mail from anywhere on the Internet. Mail is not automatically removed from the server when the user downloads it.

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

L

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

LPR (Line Printer Remote) A standard protocol for printing over TCP/IP.

M

MBONE (Multicast Backbone) A virtual network that supports IP multicasting. It uses the same physical media as the Internet, but it's designed to repackage multicast data packets so they appear to be unicast data packets.

MIME (Multipurpose Internet Mail Extension) An Internet standard for specifying what happens when a Web browser requests a file with certain characteristics. A file's suffix describes the type of file it is, and you determine how you want the server to respond when it receives files with certain suffixes. Each suffix and its associated response is called a *MIME type mapping*.

MX record (Mail Exchange record) An entry in a DNS table that specifies how mail is handled for a domain. When a mail server on the Internet has mail to deliver to a domain, it requests the MX record for the domain, and the record directs the mail to the computer specified in the MX record.

N

NetBIOS (Network Basic Input/Output System) A program that allows applications on different computers to communicate within a local area network.

NFS (Network File System) A client/server protocol that uses TCP/IP to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

NSL (Network Service Locator) The Apple technology that simplifies the search for TCP/IP-based network resources.

O

ORBS (Open Relay Behaviour-modification System) A database, accessible via DNS lookups, that tracks known spammers (senders of junk mail). The database contains SMTP servers that are known to allow third-party relay; senders of junk mail use these servers to forward their junk mail.

P

POP (Post Office Protocol) A mail protocol used to receive mail. Mail is downloaded and then stored on the user's computer.

Q

QTSS (QuickTime Streaming Server) A technology that lets you deliver media over the Internet in real time.

R

RTP (Real-Time Transport Protocol) An end-to-end network-transport protocol suitable for applications transmitting real-time data (such as audio, video, or simulation data) over multicast or unicast network services.

RTSP (Real Time Streaming Protocol) An application-level protocol for controlling the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. Sources of data can include both live data feeds and stored clips. This protocol is intended to control multiple data delivery sessions; provide a means for choosing delivery channels such as UDP, multicast UDP, and TCP; and provide a means for choosing delivery mechanisms based upon RTP.

S

SDP (Session Description Protocol) Used with QuickTime Streaming Server, an SDP file contains information about the format, timing, and authorship of the live streaming broadcast.

SLP (Service Location Protocol) DA (Directory Agent) A protocol that registers services available on a network and gives users easy access to them. When a service is added to the network, it uses SLP to register itself on the network. SLP Directory Agent (DA) is an improvement on basic SLP, using a centralized repository for registered network services.

SMB (Server Message Block) A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB to provide access to servers, printers, and other network resources.

SMTP (Simple Mail Transfer Protocol) A TCP/IP protocol used to send and transfer mail. Since its ability to queue incoming messages is limited, it is usually used only to send mail, while POP or IMAP is used to receive mail.

SSL (Secure Sockets Layer) An Internet protocol that allows you to send encrypted, authenticated information across the Internet.

T

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. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called *packets*) that a message is divided into for efficient routing through the Internet.

TTL (Time-to-Live) The specified length of time that DNS information is stored in a cache. When a domain name–IP address pair has been cached longer than the TTL value, the entry is deleted from the name server’s cache (but not from the primary DNS server).

U

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.

URL (Uniform Resource Locator) The address of a file that can be accessed on the Internet. The URL is made up of the name of the protocol needed to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

USB (Universal Serial Bus) A standard for communicating between a computer and external peripherals using an inexpensive direct-connect cable.

V

VPN (Virtual Private Network) A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

W

WebDAV (Web-based Distributed Authoring and Versioning) A live authoring environment that allows client users to check out Web pages, make changes, then check them back in while a site is running.

WINS (Windows Internet Naming Service) A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network, or externally on the Internet.

X, Y, Z

XML (Extensible Markup Language) The universal format for documents and data accessed on the Web.

Index

A

- access files for streamed media 186–187
- access logs 89, 133, 146, 179
- Access pane 134–136
- access privileges
 - client users 75
 - described 73
 - explicit 74
 - files 83
 - folders 83
 - groups 38, 86
 - guests 75, 84
 - hierarchy 75
 - for Macintosh Manager workgroups 207–210
 - media files 185–188
 - NFS exports 102–103
 - restricting 84
 - setting for WebDAV 134–136, 149
 - shared items 73–76
 - share points 38, 77, 86
 - streamed media 185–188
 - types of 74
 - user categories 74
 - users 38, 86, 201
 - Web sites 123, 124, 134–136
- Activity Log file 239
- administration 19–40
- administrator
 - adding in Macintosh Manager 197
 - logging in as 196
- logging in as user 226
- modifying account 59–60
- passwords 59–60
- return email address for 133
- workgroups 197
- Advanced pane 200–203
- AFP (Apple Filing Protocol) 85, 333
- AFP privileges 212
- AirPort technology 258
- alerts 33
- aliases, user 54–55
- All Other Users account 228
- anonymous FTP 84, 104
- Any Port filter All 299
- Apache modules 138–140
- Apache Web server
 - configuration 122, 147
 - resources 40, 150
- AppleCare Web site 243
- Apple file server 297
- Apple file service 85–92
 - configuring 85
 - described 27, 83
 - preparing for setup 85
 - problems with 91
 - settings for 86–91
 - setting up 85–86
 - specifications 92
 - starting 77, 86
- Apple Filing Protocol. *See* AFP
- Apple menu, access to 210
- AppleTalk 85, 88, 91, 112
- applications

- access to 205–207, 222
defining search policies for 56
problems with 242
- application services 30
- attributes list 270
- audio
broadcasting 181–183
live 175, 179
prerecorded 181–183
streaming 175
- authentication
LDAP-based 51
user aliases 54–55
users 41
- Authentication Manager 94
- Automount pane 80–81
- automount settings 80–81
- B**
- backups, server 328
- banner messages, for FTP 106
- Basic authentication 178, 185
- .bin (MacBinary) format 108
- BIND 280, 281
- BootP protocol 246, 248, 272
- broadcasts
audio 181–183
live 174, 175, 179–180
prerecorded 174, 181–183
starting a playlist 182
stopping a playlist 182
users connecting to 183
video 181–183
- browsing 93
- C**
- CA certificate 137, 142
- cache, DNS 169
- cache, Web server
disabling for dynamic Web pages 148–149
performance and 132
proxy servers 129
storage of 129
- CD-ROM Prefs file 239
- CD-ROMs
access to 222
ejecting 216
global settings 227
passwords 216
preferences 239
problems accessing 82
as share points 82
- certificate file 137, 143–144
- certificate signing request (CSR) 143
- CGI (Common Gateway Interface) 333
- CGI programs
enabling execution for 133, 141
installing 140
problems with 150
using 140
- Check Out pane 224
- child domains 46, 48, 49
- client computers
accessing protected media 185
access to items on 205–207
adding to NFS access list 103
AppleShare version and 85, 242
deleting 103
enabling AppleTalk 85
encoding for older clients 88
IP addresses 248
maximum connections 88, 97
setting up printing for 114
SLP DA service 265
system requirements 246
updating from Macintosh Management server 238
- client management services 28
- Client privileges for NFS 103
- client users 75, 242–243
- code page 96
- command-line interface 40
- comments, user 65, 199
- Common Gateway Interface. *See CGI*
- compressed files 107
- compression for streamed media 184
- computers
Check Out settings 224
controlling access 195

Control settings 219–220
frozen system 242
Lists settings 217–218
Log-In settings for 223–224
Security settings 221–222
tracking information in Macintosh Manager 238
Workgroups settings 218–219

Computers folder 239
Configure Web Service window 125–136
Control pane 219–220
Copy button 79
cross-platform issues for file service 93
CSR (certificate signing request) 143

D

DA (Directory Agent) 29, 267, 336
database files for Macintosh Manager 238
data types
 group information 52
 user information 52
debugging messages 270
denial-of-service attacks 294, 298
design environment 24
Desktop Admin. *See* NetBoot Desktop Admin
desktop environments 230–231
desktop printers 214
DHCP (Dynamic Host Configuration Protocol)
 described 29, 333
 enabling 277
 NetBoot clients and 248
DHCP client list 279
DHCP servers 272, 283
DHCP service 271–279
 described 29
 logs for 274, 279
 preparing for setup 271–272
 settings for 274–279
 setting up 272–274
 starting 274
 strategies 279
 uses for 271

Digest authentication 178, 185

Directory Agent (DA) 29, 266, 336

directory services 26, 41–56

Directory Setup application 51, 55–56
disconnect messages 91
discussion lists 243
Disks & Share Points window 80
DNS (Domain Name System)
 described 333
 mail service and 155
DNS servers 29, 278, 280
DNS service 280–284
 described 29
 dynamic IP addresses 283
 monitoring 283–284
 preparing for setup 280
 setting up 281
 starting 281
 strategies 282–284
 uses for 280
 using with mail service 282
DNS Statistics window 283
Documents folder 123
domain browsing services 98
domain names
 adding in mail service 159
 mail servers 158
 registering 281
 removing in mail service 159
 Web sites 131
Domain Name System. *See* DNS
domains
 See also NetInfo domains
 child 46, 48, 49
 described 42, 57
 limiting users on 50
 local 42, 46, 58
 mail service 154–155
 parent 48, 49, 279
 shared 43–45, 46, 58
drop box 74
dynamic DNS 283
Dynamic Host Configuration Protocol. *See* DHCP
dynamic IP addresses 272
dynamic Web pages 148–149

E

educational environment 21–23

email. *See mail; messages*
email, Macintosh Manager 201, 216, 220
EMBED tag 176–177
Energy Saver settings 220
environments 204
error logs 90, 134, 146, 167, 178, 270
error strings 270
Ethernet networks 247, 258
Ethernet ports 247, 253, 261
Everyone privileges 75, 79
explicit privileges 74
Extensible Markup Language. *See XML*
extensions, filename 108
Extensions folder 237

F

file formats
 exporting users/groups 308–314
 importing users/groups 308–314
 QuickTime Streaming Server 184–185
filename extensions 108
files
 access files for streamed media 186–187
 compressed 107, 184
 conversion of 107
 GIF files 148
 group files 188
 privileges 83
file services 83–109
 described 26, 83, 93
 preparing for setup 83–84
 resources 109
 types of 83
File Transfer Protocol. *See FTP*
Filter pane 161–162
filters, IP
 adding 289
 described 286–287
 IP addresses 296
 problems locating 300
 UDP ports 293
filter settings, junk mail 160–162
Find button 299
Finder environment 204, 230, 241
firewalls 163, 188

folders
 creating 77
 Documents folder 123
 Extensions folder 237
 Forced Preferences folder 235
 Global shared folder 209
 Groups folder 239
 Initial Preferences folder 234–235
 Managed Preferences folder 232
 NFS setup and 101
 Preferences folder 197
 Preserved Preferences folder 236
 Printers folder 239
 privileges 83
 sharing 101
Forced Preferences folder 235

forwarding mail 68, 160
frozen computer 242
FTP (File Transfer Protocol)
 anonymous FTP 84, 104
 connections 108
 described 27, 333
FTP servers
 banner messages 106
 security of 104, 107
 unable to connect to 108
 welcome messages 106

FTP service 104–109
 anonymous 104, 105
 configuring 104
 described 83, 106–108
 guest access 104
 preparing for setup 104
 problems with 108–109
 settings for 105
 setting up 104
 share points 104
 specifications 109
 starting 105
 strategies 106

G

General sharing settings 78–79
GIDs (group IDs) 62, 69
GIF files 148

Global pane 197–198, 225–226
Global shared folder 209
glossary 333–337
group files 188
group IDs (GIDs) 62, 69
group members 208–209
Group privileges 75, 79
groups 57–72
See also workgroups
access privileges 38, 86
adding 187
adding users to 69
characteristics of 59
characteristics of users in 69
creating 60, 68
data types for 52
defining for server 37
deleting 187
described 37, 57
editing 68
exporting 70, 308–314
file formats 308–314
importing 70, 308–314
name of 69
preparing for setup 59
primary 62
problems with 72
settings for 68–69
setting up 59–60
share point access 38
strategies 70–71
Groups folder 239
guest 84
guest access
 allowing 88, 96, 225
 described 88
 FTP service 104
 restricting 75, 84
guests
 See also users
 described 75, 84
 limiting connections 88
 maximum connections 88
 restricting access 75
guide, how to use 15–16

H

hard disk
 capacity of 247
 name of 220
help 16
higher education facilities 22–23
hint tracks 180
home directories
 creating manually 64
 default settings 36
 defining 36, 63–65, 71
 mounting automatically 70–71
 organizing 64
 real users and 107
 unable to access 243
 unable to access files in 72
 Users & Groups database 196
HTML (Hypertext Markup Language) 334
HTTP (Hypertext Transfer Protocol) 334
HTTP connections, streaming over 188
HTTP port 80 178, 188
Hypertext Markup Language (HTML) 334
Hypertext Transfer Protocol (HTTP) 334

I, J

IANA (Internet Assigned Numbers Authority) 334
ICMP (Internet Control Message Protocol) 334
ICMP echo replies 294
Idle Users pane 90–91
IGMP (Internet Group Management
Protocol) 294, 334
IMAP (Internet Message Access Protocol)
 described 154, 334
 settings for 67, 164–165
IMAP login state attribute 313
Imported Users list 228
In 43
Initial Preferences folder 234–235
Internet 304
 See also Web
Internet Assigned Numbers Authority (IANA) 334
Internet Control Message Protocol (ICMP) 334
Internet Group Management Protocol
 (IGMP) 294, 334

Internet Message Access Protocol. *See* IMAP

Internet servers. *See* Web servers

Internet service providers (ISPs) 334

InterNIC registration 281

IP addresses

assigning 272

DHCP and 271

dynamic 272

filters 296

multiple 189, 289, 305

NetBoot and 246, 248

NetInfo access 293

precedence in filters 288

ranges 288

reserved 272

setting up for ports 305

static 272

Web sites 131

IP filter list 295, 299

IP Filter module 306–307

IP filter service 285–300

adding filters 289

automatic startup 290

changing default state 299

configuring 289

described 30, 285–286

logs 297

monitoring 297

preparing for setup 286–289

problems with 300

settings for 290–296

setting up 289

starting 289

strategies 296–299

uses for 286

ipfw command 306–307

IP routing information 249–252

ISPs (Internet service providers) 334

Items pane 205–207

K

K-12 classrooms/labs 21

Kerberos authentication 225

key file 137

Knowledge Base 243

L

LDAP (Lightweight Directory Access Protocol) 42, 334

LDAP fields 52

LDAP network service data 321

LDAP search base 325

LDAP servers 51–52

authentication and 51

configuring data access 323–327

connection attributes 52

connections 326

data specifications 314–327

default mappings 322

described 42

identifying 51, 325

search policies 52

setting up 51–52, 324

stored data on 327

Lightweight Directory Access Protocol. *See* LDAP

Line Printer Remote. *See* LPR

local domains 42, 46, 58

log files

access logs 89, 133, 146, 179

error logs 90, 134, 146, 167, 178, 270

monitoring IP filter service with 297

print logs 113

queue logs 115

server logs 115

SSL logs 137

system logs 269

viewing 33

Web site logs 133

working with 269

logging in

administrator 196

Macintosh Manager 34, 241

Server Admin 31, 35

settings for 223–224

users 199

logging items

debugging messages 270

detail level of 97

DHCP activity 274

DHCP events 279

settings for 89–90, 97, 133, 178, 265, 274–275

Logging pane 97, 133

login greeting for Apple file service 87

Log-In pane 223–224

Log Viewer 33, 111, 113, 150

LPR (Line Printer Remote) 334

LPR drivers 113

LPR print jobs 115

LPR protocol 112, 116–117

M

MacBinary (.bin) format 108

Macintosh Management service 195–243

access control and 195

adding administrator 197

adding user accounts 197

database files 238

described 28, 195

email accounts 201

email addresses 220

large networks and 229

logging in as administrator 196

maximizing security 231

preferences 232–237

preparing for setup 196

problems with 241–243

resources 243

security and 237

settings for 198–227

setting up 196–198, 229, 255

starting 34, 196, 232

stopping 34

strategies 228–231

tracking information in 238

uses for 195

using with NetBoot 240

Macintosh Manager

See also computers; users; workgroups

administrator accounts 199

described 30, 34

logging in to 34

opening 34

system requirements 196

Macintosh Manager share point 239

Macintosh-specific Web modules 138

Mac OS systems

cross-platform guidelines 93

earlier versions of 232

LPR protocol 113

Mac OS X Server

accessing user information 45–46

administration of 19–40

advanced topics 301–328

described 19

information external to 45

information worksheet for 329

installation of 35

password restrictions 71

ports used by 301–304

resources 40

services included with 26–30

setting up 16, 35–39

shared data and 42–45

use in different environments 20–25

viewing information about 34

Mac OS X systems 301–304

mail

See also email; messages

bulk 164

disabling for a user 66

enabling for a user 66–67

forwarding 68, 160

incoming 166–167

NotifyMail option 67

outgoing 167–168

redirecting 282

mail accounts 66

MailAttribute field 318–320

Mail Exchange. *See* MX

mail exchangers 282

mail hosts 166–170

mail lists 243

mail servers 282

mail service 153–171

configuring 156

described 28, 153

enabling for users 66–67, 157

host settings 157, 166–170

Internet Message Access Protocol (IMAP) 154

- junk mail and 160–162
multiple domains 154–155
MX records 155
network settings 169–170
Post Office Protocol (POP) 153
preparing for setup 154–155
protocol settings 162–165
resources 170–171
settings for 65–68, 158–170
setting up 155–157
sharing 155
Simple Mail Transfer Protocol (SMTP) 154
single server 154
starting 155
using DNS service with 282
- Make 92
- MakeRefMovie tool 177
- managed preferences 233
- MBONE (Multicast Backbone) 334
- media files
- compression 184
 - controlling access to 185–188
 - copying to QuickTime Streaming Server 180–181
 - hint tracks 180
 - playlists 181–183
 - preparing for streaming 180, 181
 - problems streaming 183
 - protected 185
 - streaming and 192
- media streams
- relays 189–192
- messages
- See also* email; mail
 - automatic deletion of 160
 - blind carbon copies 159, 167
 - expired 168
 - forwarding 160
 - incoming 163
 - nondeliverable 164
 - nondelivery reports 168
 - notification 163
 - outgoing 162
 - protocols for 162–163
 - settings for 159–160
- spam and 160–162
Messages pane 159–160
MIME (Multipurpose Internet Mail Extension) 141–142, 334
- MIME suffixes 141
- MIME type editor 142
- MIME type mapping 141
- MIME types 128
- MIME Types pane 128
- mod_auth_apple module 139
- mod_hfs_apple module 139
- mod_macbinary_apple module 138
- mod_perl module 140
- mod_redirectacgi_apple module 139
- mod_sherlock_apple module 138
- movies 177, 181
- Movies directory 177
- Multicast Backbone (MBONE) 334
- multicast streams 189
- Multipurpose Internet Mail Extension. *See* MIME
- Multi-User Items file 239
- Multi-User Items folder 238, 239
- MX (Mail Exchange) records 155, 281, 282, 335
- MX hosts 282
- MySQL module 140

N

- name servers 29, 280
- Neighborhood pane 98
- Neighborhood settings 98
- NetBIOS (Network Basic Input/Output System) 335
- NetBoot 245–261
- AirPort technology and 258
 - client computer startup 255
 - described 28, 245
 - installing software for 254
 - performance 257–260
 - preparing for setup 246–253
 - problems with 261
 - server worksheet 253
 - setting up 254–255
 - strategies 257–260
 - system requirements 246–247
 - uses for 245

- using Macintosh Manager with 240
- NetBoot clients
- connected to server 246–247
 - list of 279
 - performance 259
- NetBoot Desktop Admin 31, 35, 255–257
- NetBoot HD disk image 256–257
- NetBoot servers 253–255
- NetBoot Setup Assistant 247–252, 254
- NetInfo domains 46–50
- See also* domains
 - adding 59
 - configuring 70
 - creating ??–50
 - designing hierarchies 50
 - multilevel hierarchies 49
 - searching through hierarchies 49
 - search policies 52
 - settings for 291–293
 - setting up 50
 - sharing and 46
 - stored data on 42
 - two-level hierarchies 46–48
- NetInfo pane in DHCP service 278–279
- NetInfo parent domain 279
- NetInfo server tag 278
- Network Basic Input/Output System (NetBIOS) 335
- Network File System. *See* NFS
- Network Neighborhood 99
- networks
- Ethernet network speed 258
 - management resources 40
 - NetBoot performance 258
 - planning 246–252
 - scopes 264, 265–266
 - setting up workgroups on 229–230
 - sharing printer queues over 112–113
 - streaming media and 188
 - TCP/IP networks 304–308
- Network Service Locator (NSL) 335
- network services
- assigning to scopes 266
 - described 263
 - included with Mac OS X Server 28
- mapping data 321
- resources for 300
- NFS (Network File System) 81, 335
- NFS Access Control pane 81, 102
- nfsd daemons 101
- NFS service 100–103
- access control settings 102–103
 - configuring 101
 - described 27, 83
 - folder sharing 101
 - preparing for setup 100
 - settings for 101–103
 - setting up 101
 - uses for 100
- nobody user 103
- None privilege 74
- NotifyMail option 67
- NSL (Network Service Locator) 335

O

- online help 16
- Open Relay Behaviour-modification System. *See* ORBS
- open source modules 139–140
- Options pane 215–216
- ORBS (Open Relay Behaviour-modification System) 335
- ORBS servers 160, 161
- Owner privileges 75, 78

P

- packet logging 291
- Panels environment 204, 231
- parent-child hierarchies 46–49
- parent domains 48, 49, 278, 279
- Password data type 52
- passwords
- administrator 59–60
 - authentication and 41
 - cleartext 94, 99
 - ejecting CD-ROMs 216
 - encrypted 94
 - file servers 92
 - for printing 214

printers 214
restrictions on 71
root user 59–60
users 37, 61, 226
Windows systems 94

performance
cache and 132
monitoring 146–147
NetBoot clients 257–258, 259
NetBoot networks 258
NetBoot server 258–260
persistent connections and 137
streaming 193

persistent connections 137

PHP module 140

playlists 181–183

POP (Post Office Protocol) 67, 153, 335

POP3 login state attribute 313

POP3 settings 165

port 80 178, 188

ports
Ethernet ports 247, 253, 261
for Web sites 132
HTTP ports 178
IP addresses 247, 305
Mac OS X computers 301–304
name 296
number 296
SMTP ports 170
subnet ports 276
TCP ports 301–303
UDP ports 293, 303

postmaster account 157

Post Office Protocol. *See* POP

PostScript-compatible printers 111–119, 213

preferences
administrator-defined 198
CD-ROMs 239
forced 235
initial 234–235
Internet 198
Macintosh Manager and 197, 232–237
managed 233
preserved 236–237
storage of 232–233

user 226, 233

Preferences folder 197

Preserved Preferences folder 236

Print Center 111, 114

printers
adding 114
connecting to server 111–112
limiting use of 214
passwords 214
sharing 111–119

Printers folder 239

Printers pane 213–214

printing 114

print jobs
holding 117, 118
managing 113
monitoring 113
priority of 117, 118
settings for 117–118

print logs 113

Print module 111, 113

Print Monitor 113, 116

print queues
configuring 114
LPR protocol 116–117
managing 113
names of 116
settings for 116–117
sharing 112–113, 116–117

print service 111–119
configuring 114
described 27, 93, 111
preparing for setup 113
problems with 118–119
settings for 115–118
setting up 114
starting 114

privileges. *See* access privileges

Privileges pane 207–210

Privileges pop-up menu 79

problems. *See* troubleshooting

Protocols pane 162–163

Proxy pane 129–130

proxy servers 129–130

proxy settings 129–130

publishing environment 24

Q

qtaccess file 187
QTSS. *See* QuickTime Streaming Server
QTSSAccessModule 185
queue logs 115
Queue Monitor 113
QuickTime 5 173, 174, 178, 185
QuickTime client software 174
QuickTime Player 173, 180
QuickTime Plugin 173, 183
QuickTime Pro 180
QuickTime Streaming Server (QTSS) 173–194
 address translation 188
 compatible file formats 184–185
 controlling access to steam media 185–188
 copying media files to 180–181
 described 28, 173, 335
 features of 173
 preparing for setup 174–175
 preparing media files for 181
 problems with 192–193
 relays 189–192
 resources 194
 settings for 176, 177–179
 setting up 175–177
 strategies 179–183
 system requirements 174
 users connected to 179
 uses for 174
 viewing streamed media 173–174
QuickTime Web site 180

R

Read & Write privileges 74
README messages, for FTP 106
Read Only privileges 74, 103
realms, WebDAV 135, 149
RealName data type 52
Real Time Streaming Protocol (RTSP) 335
Real-Time Transport Protocol (RTP) 335
RecordName data type 52
reference movies 177, 181

Registered Services window 268–269

relay configuration files 190–192
relays, media streams 189–192
removable media 209

Request for Comments (RFC) documents 170
resources

 Apache Web server 40
 file services 109
 Macintosh Management service 243
 Mac OS X Server 40
 mail service 170–171
 network management 40
 network services 300
 QuickTime Streaming Server 194
 TCP/IP 308
 Web service 151
 XML 314

Restricted Finder environment 204, 231

RFC (Request for Comments) documents 170
root password 59–60
routers 265, 277
RTP (Real-Time Transport Protocol) 335
RTSP (Real Time Streaming Protocol) 335
rules, IP filter 306–307

S

scopes, network 264, 265–266, 268
scripts, CGI 140
SDP (Session Description Protocol) 174, 336
search policies 52–56
 custom 50, 54
 default 52
 defining for personal applications 56
 defining for server 56
 described 46
 LDAP servers 52
 NetInfo domains 52
 setting up 55–56
Secure Sockets Layer. *See* SSL
security 75–76
 client computer settings 208, 221–222
 file sharing precautions 84
 FTP servers 104, 107
 global settings 225–226
 limiting user actions 221

- Macintosh Manager and 237
maximizing 231
NFS exports and 100
options for 197–198
restricting file access 75
secure Web transactions 136–137
WebDAV 123
Web sites 123
- Security pane 136–137, 221–222
serial number, server 34
- Server Admin 31–34
described 30
logging in to 31, 35
toolbar 32–33
- server logs 115
- Server Message Block (SMB) 336
- servers
- See also* LDAP servers; Mac OS X Server; QuickTime Streaming Server
- Apache Web server 40, 122, 147
backing up 328
browsing for 93
connecting printers to 111–112
DHCP servers 283
DNS servers 29, 278
enabling SSL on 144–146
file servers 91
FTP servers 104, 106, 108
LDAP servers 51–52, 324
mail account on 66
monitoring activity 146–147
multiple IP addresses 189
name of 86, 95
name servers 29, 280
NetBoot clients connected to 246–247
NetBoot servers 253–255
ORBS servers 160, 161
performance 137, 146–147, 258–260
proxy servers 129–130
quits unexpectedly 192
serial number of 34
setting up share points on 70
SMTP servers 162
unable to log in to 242
unable to start 192
- updating clients from 238
users administering 37, 62
users logging in to 62
Windows file servers 95
WINS servers 98
- Service Location Protocol. *See* SLP
- service modules 32–33
- services
- See also specific services*
- administering 30–35
deregistered 267
expirations 267
included with Mac OS X Server 26–30
registered 267, 269
requests 267
setting up additional services 38–39
user data required by 41
- Session Description Protocol (SDP) 174, 336
- settings
- Apple file service 86–91
automount 80–81
connected users 179
FTP service 105
general sharing 78–79
groups 68–69
home directories 36
junk mail 160–162
logging 89–90, 97, 133, 178, 265, 274–275
Macintosh Management service 198–227
mail service 65–68, 158–170
messages 159–160
MIME types 128
NetInfo 291–293
networks 169–170
NFS Access Control 81
NFS service 101–103
print service 115–118
proxy 129–130
QuickTime Streaming Server 176, 177–179
security 136–137
subnets 275–279
users 60–68
Web service 125–136
Web sites 127, 130–136
Windows services 95–98

shared domains 43–??, 43–45, 46, 58
share points
 access privileges 38
 CD-ROMs as 82
 creating 36, 77
 described 36, 73
 FTP service 104
 Macintosh Manager 239
 multiple 229
 setting privileges for 77
 setting up on server 70
sharing
 files/volumes 73–82
 folders 101
 mail service 155
 network data 42–45
 printers 111–119
 print queues 116–117
 privileges 73–76
 problems with 82
 settings for 78–81
 setting up 76–77
Sharing module 73–82
sharing window 78–81
Simple Mail Transfer Protocol. *See* SMTP
site settings window 130–138
SLP (Service Location Protocol) 29, 87, 336
SLP DA service 264–270
 preparing for setup 264
 settings for 267–269
 setting up 265–266
 starting 266
 strategies 269–270
 uses for 264
SLP Directory Agent (DA) 29, 336
SMB (Server Message Block) 336
SMB protocol 93, 113
SMTP (Simple Mail Transfer Protocol)
 connections 161
 described 154, 336
 names 161
 settings 163–164
SMTP ports 170
SMTP relay 164, 166, 168
SMTP servers 162
specifications
 Apple file service 92
 FTP service 109
 LDAP data 314–327
 Web service 150
 Windows services 99
SSL (Secure Sockets Layer)
 described 122, 336
 enabling 126, 136, 144–146
SSL (Secure Sockets Layer) service 142–146
SSL log file 137
SSL pass phrase 137
static IP addresses 272
streaming media
 address translation 188
 controlling access to 185–188
 firewalls and 188
 in Web pages 176–177
 live audio/video 175, 179
 multicast streams 189
 multiple sources 181
 networks and 188
 on port 80 188
 performance of 193
 unicast streams 189
 viewing 173–174
Streaming Server Admin 175–176
 described 31, 34
 not responding 192
 opening 34, 176
subnet masks 247, 276, 287, 296
subnet ports 276
subnets
 creating 271, 273–274
 settings for 275–279
system logs 269

T

TCP (Transmission Control Protocol) 102, 336
TCP/IP
 advanced topics 301–308
 private networks 304
 resources for 308
 unable to access server over 300
TCP ports 301–303

Telnet connections 63
Terminal application 40, 307
The 73, 169
timeouts 126, 170
Time to Live (TTL) 336
Tomcat module 139
Transmission Control Protocol (TCP) 102, 336
troubleshooting
 Apple file service 91
 applications 242
 client users 242–243
 denial-of-service attacks 298
 frozen system 242
 FTP service 108–109
 groups 72
 IP filters 300
 Macintosh Management service 241–243
 NetBoot 261
 playlists 183
 print service 118–119
 QuickTime Streaming Server 192–193
 sharing problems 82
 users 72
 Web service 149–150
 Windows services 99
TTL (Time to Live) 336
tunneling 265

U

UDP (User Datagram Protocol) 102, 336
UDP packets 188
UDP ports 293, 303
unicast streams 189
Unicode 85, 93
UniqueID data type 52
Universal Serial Bus (USB) 112, 336
UNIX systems 113
unregistered users. *See* guests
URLs (Uniform Resource Locators) 336
USB (Universal Serial Bus) 112, 336
user accounts 197, 199
User Datagram Protocol. *See* UDP
user files 188
user IDs 41, 62
users 57–72

See also guests
accessing information about 45–46
accessing protected media 185
access privileges 38, 86, 201, 207–210
access to Macintosh Manager 228
adding to groups 69, 203–204
adding to user files for streaming access 187
administering server 37, 62
advanced Macintosh Manager
 settings 200–203
aliases 54–55
anonymous FTP users 108
authentication 41
automatic disconnection 70
basic Macintosh Manager settings 198–199
categories 74
characteristics of 58
client users 75
comments 65, 199
connected to streaming server 179
connecting to broadcasts 183
creating 60
data required by services 41
data types for 52
defining for server 36–37
defining home directories for 63–65, 71
defining in local domain 42
described 57
disabling mail service for 66
editing 60
enabling mail service for 66–67, 157
exporting 70, 308–314
file formats 308–314
forwarding mail for 68
importing 70, 308–314
information about 57–58
limiting connections 88
limits on domain users 50
logging in 62, 199
login shell for 63
mapping data 103, 315–320
maximum number of streaming
 connections 178
name of 37, 41, 61, 199
passwords 37, 61, 226

preferences 226, 233
preparing for setup 59
problems with 72
real vs. anonymous 107
registered 84
security settings 221
settings for 60–68
setting up 59–60
shared data and 42–45
share point access 38
strategies 70–71
tracking information in Macintosh
 Manager 238
types of 199
unable to log in 72
unregistered 75

Users & Groups database 196
Users & Groups module 57–72, 308
users and groups file 312–314
Users folder 239

V, W

video
 broadcasting 181–183
 live 175, 179
 prerecorded 181–183
 streaming 175

Virtual Private Networks (VPNs) 337

Volumes pane 211–212

VPNs (Virtual Private Networks) 337

Web-based Distributed Authoring and Versioning.
 See WebDAV

Web browsers 123

WebDAV (Web-based Distributed Authoring and Versioning)
 defining realms 149
 described 121, 337
 enabling 126, 132
 security 123
 setting access privileges 149

Web modules 138–140

WebObjects 30

Web pages
 default 124
 disabling cache 148–149

dynamic 148–149
playing streamed media through 173
streamed media in 176–177

Web servers
 See also servers
 Apache Web server 40, 122, 147
 certificate for 144
 connection timeouts 126
 maximum requests 126
 persistent connections 126

Web service 121–151
 configuring 122, 124
 default page 124
 described 27, 121
 Documents folder 123
 monitoring server activity 146–147
 preparing for setup 121–123
 problems with 149–150
 resources 151
 secure transactions 122, 142–146
 server performance 146–147
 settings for 125–136
 setting up 123–124
 setting up Web sites 122
 specifications 150
 starting 124
 strategies for 137–149
 tools 146–147
 Web site privileges 124

Web service providers 25

Web Service Status window 146

Web sites
 access privileges 123
 access settings 134–136
 adding 127
 Apache Web server 40
 AppleCare 243
 assigning privileges 124
 connecting to 124
 connection problems 149
 default page 124
 deleting 127
 directories for 132
 domain names 131
 duplicating 127

editing 127
hosting 122–123, 124
information about 127
IP addresses 131
maximum number of connections 126
path to 135
persistent connections 126, 137
QuickTime 180
QuickTime client software 174
security of 123
settings for 127, 130–136
setting up 122
turning on/off 127
welcome messages for FTP 106
When 140
Windows clients 93, 95
Windows file servers 95
Windows Internet Naming Service. *See* WINS
Windows servers 95–98
Windows services 93–99
 configuring 94
 described 27, 83
 enabling printing 114
 preparing for setup 93–94
 problems with 99
 settings for 95–98
 setting up 94
 specifications 99
 starting 95
Windows systems
 cross-platform guidelines 93
 LPR protocol 113
 password validation 94
 printing and 114, 115
Windows users
 enabling printing for 114
 unable to log in 99
WINS (Windows Internet Naming Service) 93,
 337
WINS servers 98
workgroup administrator accounts 199
workgroup administrators 197
Workgroup hand-in folder 209
workgroups
 computer access 218
creating 197
desktop environments 230–231
Items settings 205–207
Members settings 203–204
name of 203
Options settings 215–216
Printers settings 213–214
Privileges settings 207–210
restricting computers to 218–219
setting up 229–230
tracking information in Macintosh
 Manager 238
volumes settings 211–212
Windows name 96
Workgroup shared folder 209
Workgroups pane 203–204, 230
worksheet, Mac OS X Server 329
workstation security 208
World privileges for NFS 75, 103
Write Only privileges 74

X, Y, Z

XML (Extensible Markup Language)
 described 337
 example file 308–311
 resources for 314
XML files 312–314