

Mac OS X Server
Administrator's Guide

 **Apple Computer, Inc.**

© 2002 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, AppleFalk, ColorSync, 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, 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.

062-9285/7-26-02



Contents

Preface

How to Use This Guide 39

- What's Included in This Guide 39
- Using This Guide 40
- Setting Up Mac OS X Server for the First Time 41
- Getting Help for Everyday Management Tasks 41
- Getting Additional Information 41

1 Administering Your Server 43

- Highlighting Key Features 43
 - Ease of Setup and Administration 43
 - Networking and Security 44
 - File and Printer Sharing 44
 - Open Directory Services 45
 - Comprehensive Management of Macintosh Workgroups 45
 - High Availability 46
 - Extensive Internet and Web Services 46
- Highlighting Individual Services 46
 - Directory Services 47
 - Open Directory 47
 - Password Validation 47
 - Search Policies 48
 - File Services 48
 - Sharing 48
 - Apple File Service 49
 - Windows Services 49

Network File System (NFS) Service	49
File Transfer Protocol (FTP)	50
Print Service	50
Web Service	51
Mail Service	51
Macintosh Workgroup Management	52
Client Management	52
NetBoot	52
Network Install	53
Network Services	53
DHCP	54
DNS	54
IP Firewall	54
SLP DA	54
QuickTime Streaming Service	55
Highlighting Server Applications	56
Administering a Server From Different Computers	58
Server Assistant	58
Open Directory Assistant	58
Directory Access	59
Workgroup Manager	59
Opening and Authenticating in Workgroup Manager	59
Major Workgroup Manager Tasks	60
Server Settings	60
Server Status	61
Macintosh Manager	62
NetBoot Administration Tools	62
Network Install Administration Application	62
Server Monitor	62
Streaming Server Admin	63
Where to Find More Information	64
If You're New to Server and Network Management	64
If You're an Experienced Server Administrator	64

2 Directory Services 65

Storage for Data Needed by Mac OS X	66
A Historical Perspective	67
Data Consolidation	68
Data Distribution	69
Uses of Directory Data	70
Inside a Directory Domain	71
Discovery of Network Services	72
Directory Domain Protocols	73
Local and Shared Directory Domains	74
Local Data	74
Shared Data	75
Shared Data in Existing Directory Domains	78
Directory Domain Hierarchies	78
Two-Level Hierarchies	79
More Complex Hierarchies	81
Search Policies for Directory Domain Hierarchies	82
The Automatic Search Policy	83
Custom Search Policies	84
Directory Domain Planning	85
General Planning Guidelines	85
Controlling Data Accessibility	86
Simplifying Changes to Data in Directory Domains	86
Identifying Computers for Hosting Shared Domains	87
Open Directory Password Server	87
Authentication With a Password Server	88
Network Authentication Protocols	88
Password Server Database	88
Password Server Security	89
Overview of Directory Services Tools	89
Setup Overview	90
Before You Begin	91
Setting Up an Open Directory Domain and Password Server	92
Deleting a Shared Open Directory Domain	93

Configuring Open Directory Service Protocols	93
Setting Up Search Policies	94
Using the Automatic Search Policy	95
Defining a Custom Search Policy	95
Using a Local Directory Search Policy	96
Changing Basic LDAPv3 Settings	97
Enabling or Disabling Use of DHCP-Supplied LDAPv3 Servers	97
Showing or Hiding Available LDAPv3 Configurations	97
Configuring Access to Existing LDAPv3 Servers	98
Creating an LDAPv3 Configuration	98
Editing an LDAPv3 Configuration	99
Duplicating an LDAPv3 Configuration	99
Deleting an LDAPv3 Configuration	100
Changing an LDAPv3 Configuration's Connection Settings	100
Configuring LDAPv3 Search Bases and Mappings	101
Populating LDAPv3 Domains With Data for Mac OS X	103
Using an Active Directory Server	104
Creating an Active Directory Server Configuration	104
Setting Up an Active Directory Server	105
Populating Active Directory Domains With Data for Mac OS X	105
Accessing an Existing LDAPv2 Directory	106
Setting Up an LDAPv2 Server	106
Creating an LDAPv2 Server Configuration	106
Changing LDAPv2 Server Access Settings	107
Editing LDAPv2 Search Bases and Data Mappings	108
Using NetInfo Domains	110
Creating a Shared NetInfo Domain	110
Configuring NetInfo Binding	111
Adding a Machine Record to a Parent NetInfo Domain	113
Configuring Static Ports for Shared NetInfo Domains	113
Viewing and Changing NetInfo Data	114
Using UNIX Utilities for NetInfo	114
Using Berkeley Software Distribution (BSD) Configuration Files	115
Mapping BSD Configuration Files	115

Setting Up Data in BSD Configuration Files	118
Configuring Directory Access on a Remote Computer	118
Monitoring Directory Services	119
Backing Up and Restoring Directory Services Files	119

3 Users and Groups 121

How User Accounts Are Used	122
Authentication	122
Password Validation	123
Information Access Control	124
Directory and File Owner Access	125
Directory and File Access by Other Users	125
Administration Privileges	125
Server Administration	125
Local Mac OS X Computer Administration	126
Directory Domain Administration	126
Home Directories	126
Mail Settings	127
Resource Usage	127
User Preferences	127
How Group Accounts Are Used	127
Information Access Control	127
Group Directories	128
Workgroups	128
Computer Access	128
Kinds of Users and Groups	128
Users and Managed Users	128
Groups, Primary Groups, and Workgroups	129
Administrators	129
Guest Users	129
Predefined Accounts	130
Setup Overview	132
Before You Begin	135
Administering User Accounts	137
Where User Accounts Are Stored	137

Creating User Accounts in Directory Domains on Mac OS X Server	137
Creating Read-Write LDAPv3 User Accounts	138
Changing User Accounts	138
Working With Read-Only User Accounts	139
Working With Basic Settings for Users	139
Defining User Names	139
Defining Short Names	140
Choosing Stable Short Names	141
Avoiding Duplicate Names	141
Avoiding Duplicate Short Names	143
Defining User IDs	144
Defining Passwords	145
Assigning Administrator Rights for a Server	145
Assigning Administrator Rights for a Directory Domain	145
Working With Advanced Settings for Users	146
Defining Login Settings	146
Defining a Password Validation Strategy	147
Editing Comments	147
Working With Group Settings for Users	147
Defining a User's Primary Group	148
Adding a User to Groups	148
Removing a User From a Group	149
Reviewing a User's Group Memberships	149
Working With Home Settings for Users	149
Working With Mail Settings for Users	150
Disabling a User's Mail Service	150
Enabling Mail Service Account Options	150
Forwarding a User's Mail	151
Working With Print Settings for Users	151
Disabling a User's Access to Print Queues Enforcing Quotas	152
Enabling a User's Access to Print Queues Enforcing Quotas	152
Deleting a User's Print Quota for a Specific Queue	153
Restarting a User's Print Quota	153
Working With Managed Users	154

Defining a Guest User	154
Deleting a User Account	154
Disabling a User Account	155
Administering Home Directories	155
Distributing Home Directories Across Multiple Servers	156
Setting Up Home Directories for Users Defined in Existing Directory Servers	157
Choosing a Protocol for Home Directories	160
Setting Up AFP Home Directory Share Points	160
Setting Up NFS Home Directory Share Points	160
Creating Home Directory Folders	161
Defining a User's Home Directory	161
Defining No Home Directory	162
Defining a Home Directory for Local Users	162
Defining a Network Home Directory	163
Defining an Advanced Home Directory	163
Setting Disk Quotas	164
Defining Default Home Directories for New Users	165
Using Import Files to Create AFP Home Directories	165
Moving Home Directories	165
Deleting Home Directories	165
Administering Group Accounts	165
Where Group Accounts Are Stored	165
Creating Group Accounts in a Directory Domain on Mac OS X Server	165
Creating Read-Write LDAPv3 Group Accounts	166
Changing Group Accounts	167
Working With Read-Only Group Accounts	167
Working With Member Settings for Groups	167
Adding Users to a Group	168
Removing Users From a Group	168
Naming a Group	169
Defining a Group ID	170
Working With Volume Settings for Groups	170
Creating Group Directories	171
Automatically Creating Group Directories	171

Customizing Group Directory Settings	172
Working With Group and Computer Preferences	173
Deleting a Group Account	173
Finding User and Group Accounts	173
Listing Users and Groups in the Local Directory Domain	174
Listing Users and Groups in Search Path Directory Domains	174
Listing Users and Groups in Available Directory Domains	174
Refreshing User and Group Lists	175
Finding Specific Users and Groups in a List	175
Sorting User and Group Lists	175
Shortcuts for Working With Users and Groups	176
Editing Multiple Users Simultaneously	176
Using Presets	176
Creating a Preset for User Accounts	176
Creating a Preset for Group Accounts	177
Using Presets to Create New Accounts	177
Renaming Presets	178
Deleting a Preset	178
Changing Presets	178
Importing and Exporting User and Group Information	178
Understanding What You Can Import	179
Using Workgroup Manager to Import Users and Groups	179
Using Workgroup Manager to Export Users and Groups	181
Using dsimportexport to Import Users and Groups	181
Using dsimportexport to Export Users and Groups	184
Using XML Files Created With Mac OS X Server 10.1 or Earlier	186
Using XML Files Created With AppleShare IP 6.3	186
Using Character-Delimited Files	187
Writing a Record Description	188
Using the StandardUserRecord Shorthand	189
Using the StandardGroupRecord Shorthand	189
Understanding Password Validation	189
Contrasting Password Validation Options	191
The Authentication Authority Attribute	192

Choosing a Password	192
Migrating Passwords	193
Setting Up Password Validation Options	193
Storing Passwords in User Accounts	193
Enabling Basic Password Validation for a User	193
The Problem With Readable Passwords	194
Using a Password Server	195
Setting Up a Password Server	196
Enabling the Use of a Password Server for a User	196
Exporting Users With Password Server Passwords	197
Making a Password Server More Secure	197
Monitoring a Password Server	197
Using Kerberos	197
Understanding Kerberos	198
Integrating Mac OS X With a Kerberos Server	199
Enabling Kerberos Authentication for Mail	200
Enabling Kerberos Authentication for AFP	200
Enabling Kerberos Authentication for FTP	200
Enabling Kerberos Authentication for Login Window	200
Enabling Kerberos Authentication for Telnet	201
Solving Problems With Kerberos	201
Using LDAP Bind Authentication	201
Backing Up and Restoring Files	201
Backing Up a Password Server	201
Backing Up Root and Administrator User Accounts	202
Supporting Client Computers	202
Validating Windows User Passwords	202
Setting Up Search Policies on Mac OS X Client Computers	202
Solving Problems	202
You Can't Modify an Account Using Workgroup Manager	202
A Password Server User's Password Can't Be Modified	203
Users Can't Log In or Authenticate	203
You Can't Assign Server Administrator Privileges	204
Users Can't Access Their Home Directories	204

Mac OS X User in Shared NetInfo Domain Can't Log In	204
Kerberos Users Can't Authenticate	204

4 Sharing 205

Privileges	205
Explicit Privileges	206
User Categories	206
Privileges Hierarchy	207
Client Users and Privileges	207
Privileges in the Mac OS X Environment	207
Network Globe Contents	207
Share Points in the Network Globe	208
Static Versus Dynamic Linking	208
Adding System Resources to the Network Library Folder	208
Setup Overview	208
Before You Begin	209
Organize Your Shared Information	210
Windows Users	210
Security Issues	210
Restricting Access by Unregistered Users (Guests)	210
Setting Up Sharing	211
Creating Share Points and Setting Privileges	211
Configuring Apple File Protocol (AFP) Share Points	212
Configuring Server Message Block (SMB) Share Points	212
Configuring File Transfer Protocol (FTP) Share Points	213
Sharing (Exporting) Items Using Network File System (NFS)	213
Automounting Share Points	214
Resharing NFS Mounts as AFP Share Points	215
Managing Sharing	215
Turning Sharing Off	216
Removing a Share Point	216
Browsing Server Disks	216
Viewing Share Points	216
Copying Privileges to Enclosed Items	217
Viewing Share Point Settings	217

Changing Share Point Owner and Privilege Settings	217
Changing the Protocols for a Share Point	218
Deleting an NFS Client from a Share Point	218
Creating a Drop Box	218
Supporting Client Computers	219
Solving Problems	219
Users Can't Access a CD-ROM Disc	219
Users Can't Find a Shared Item	219
Users Can't See the Contents of a Share Point	219

5 File Services 221

Before You Begin	221
Security Issues	222
Allowing Access to Registered Users Only	222
Client Computer Requirements	223
Setup Overview	223
Apple File Service	224
Automatic Reconnect	224
Find By Content	224
Kerberos Authentication	224
Apple File Service Specifications	224
Before You Set Up Apple File Service	225
Setting Up Apple File Service	225
Configuring Apple File Service General Settings	225
Configuring Apple File Service Access Settings	226
Configuring Apple File Service Logging Settings	227
Configuring Apple File Service Idle Users Settings	228
Starting Apple File Service	229
Managing Apple File Service	229
Viewing Apple File Service Status	229
Viewing Apple File Service Logs	230
Stopping Apple File Service	230
Starting Up Apple File Service Automatically	231
Changing the Apple File Server Name	231
Registering With Network Service Locator	231

Enabling AppleTalk Browsing for Apple File Service	232
Setting Maximum Connections for Apple File Service	232
Turning On Access Logs for Apple File Service	232
Archiving Apple File Service Logs	233
Disconnecting a User From the Apple File Server	233
Disconnecting Idle Users From the Apple File Server	234
Allowing Guest Access to the Apple File Server	234
Creating a Login Greeting for Apple File Service	234
Sending a Message to an Apple File Service User	235
Windows Services	235
Windows Services Specifications	236
Before You Set Up Windows Services	236
Ensuring the Best Cross-Platform Experience	236
Windows User Password Validation	236
Setting Up Windows Services	237
Configuring Windows Services General Settings	237
Configuring Windows Services Access Settings	238
Configuring Windows Services Logging Settings	239
Configuring Windows Services Neighborhood Settings	239
Starting Windows Services	240
Managing Windows Services	240
Stopping Windows Services	240
Setting Automatic Startup for Windows Services	240
Changing the Windows Server Name	241
Finding the Server's Workgroup Name	241
Checking Windows Services Status	241
Registering with a WINS Server	242
Enabling Domain Browsing for Windows Services	242
Setting Maximum Connections for Windows Services	242
Setting Up the Windows Services Log	243
Disconnecting a User From the Windows Server	243
Allowing Guest Access in Windows Services	243
Assigning the Windows Server to a Workgroup	244
File Transfer Protocol (FTP) Service	244

Secure FTP Environment	244
User Environments	245
On-the-Fly File Conversion	247
Custom FTP Root	248
Kerberos Authentication	248
Before You Set Up FTP Service	248
Restrictions on Anonymous FTP Users (Guests)	249
Setup Overview	249
Setting Up File Transfer Protocol (FTP) Service	250
Configuring FTP General Settings	250
Configuring FTP Access Settings	251
Configuring FTP Logging Settings	251
Configuring FTP Advanced Settings	252
Starting FTP Service	252
Managing File Transfer Protocol (FTP) Service	252
Stopping FTP Service	252
Setting Up Anonymous FTP Service	253
Creating an Uploads Folder for Anonymous Users	253
Specifying a Custom FTP Root	253
Specifying the FTP Authentication Method	254
Configuring the FTP User Environment	254
Viewing FTP Logs	254
Displaying Banner and Welcome Messages to Users	255
Displaying Messages Using message.txt files	255
Using README Message	255
Network File System (NFS) Service	256
Before You Set Up NFS Service	256
Security Implications	256
Setup Overview	256
Setting Up NFS Service	257
Configuring NFS Settings	257
Managing NFS Service	258
Stopping NFS Service	258
Viewing NFS Service Status	258

Viewing Current NFS Exports	258
Supporting Client Computers	259
Supporting Mac OS X Clients	259
Connecting to the Apple File Server in Mac OS X	259
Setting Up a Mac OS X Client to Mount a Share Point Automatically	260
Changing the Priority of Network Connections	260
Supporting Mac OS 8 and Mac OS 9 Clients	260
Connecting to the Apple File Server in Mac OS 8 or Mac OS 9	261
Setting up a Mac OS 8 or Mac OS 9 Client to Mount a Share Point Automatically	261
Supporting Windows Clients	261
TCP/IP	262
Using the Network Neighborhood to Connect to the Windows Server	262
Connecting to the Windows Server Without the Network Neighborhood	262
Supporting NFS Clients	262
Solving Problems With File Services	263
Solving Problems With Apple File Service	263
User Can't Find the Apple File Server	263
User Can't Connect to the Apple File Server	263
User Doesn't See Login Greeting	263
Solving Problems With Windows Services	263
User Can't See the Windows Server in the Network Neighborhood	263
User Can't Log in to the Windows Server	264
Solving Problems With File Transfer Protocol (FTP)	264
FTP Connections Are Refused	264
Clients Can't Connect to the FTP Server	265
Anonymous FTP Users Can't Connect	265
Where to Find More Information About File Services	265

6 Client Management: Mac OS X 267

The User Experience	268
Logging In	268
Locating the Home Directory	268
Before You Begin	269
Designating Administrators	270
Setting Up User Accounts	270

Setting Up Group Accounts	271
Setting Up Computer Accounts	271
Creating a Computer Account	272
Creating a Preset for Computer Accounts	273
Using a Computer Accounts Preset	273
Adding Computers to an Existing Computer Account	274
Editing Information About a Computer	274
Moving a Computer to a Different Computer Account	275
Deleting Computers From a Computer List	275
Deleting a Computer Account	276
Searching for Computer Accounts	276
Managing Guest Computers	277
Working With Access Settings	278
Restricting Access to Computers	278
Making Computers Available to All Users	279
Using Local User Accounts	279
Managing Portable Computers	280
Unknown Portable Computers	280
Portable Computers With Multiple Local Users	280
Portable Computers With One Primary Local User	280
Using Wireless Services	281
How Workgroup Manager Works With System Preferences	281
Managing Preferences	282
About the Preferences Cache	283
Updating the Managed Preferences Cache	283
Updating Cached Preferences Manually	283
How Preference Management Works	284
Preference Management Options	284
Managing a Preference Once	285
Always Managing a Preference	285
Never Managing a Preference	285
Managing User Preferences	285
Managing Group Preferences	286
Managing Computer Preferences	286

Editing Preferences for Multiple Records	287
Disabling Management for Specific Preferences	287
Managing Applications Preferences	288
Applications Items Preferences	288
Creating a List of Approved Applications	288
Preventing Users From Opening Applications on Local Volumes	289
Managing Application Access to Helper Applications	289
Applications System Preferences	290
Managing Access to System Preferences	290
Managing Classic Preferences	291
Classic Startup Preferences	291
Making Classic Start Up After a User Logs In	291
Choosing a Classic System Folder	291
Classic Advanced Preferences	292
Allowing Special Actions During Restart	292
Keeping Control Panels Secure	292
Preventing Access to the Chooser and Network Browser	293
Making Apple Menu Items Available in Classic	293
Adjusting Classic Sleep Settings	294
Managing Dock Preferences	294
Dock Display Preferences	294
Controlling the User's Dock	294
Dock Items Preferences	295
Adding Items to a User's Dock	295
Preventing Users From Adding Additional Dock Items	296
Managing Finder Preferences	296
Finder Preferences	296
Keeping Disks and Servers From Appearing on the User's Desktop	296
Controlling the Behavior of Finder Windows	297
Making File Extensions Visible	298
Selecting the User Environment	298
Hiding the Alert Message When a User Empties the Trash	298
Finder Commands Preferences	299
Controlling User Access to an iDisk	299

Controlling User Access to Remote Servers	299
Controlling User Access to Folders	300
Preventing Users From Ejecting Disks	300
Hiding the Burn Disc Command in the Finder	301
Removing Restart and Shut Down Commands From the Apple Menu	301
Finder Views Preferences	302
Adjusting the Appearance and Arrangement of Desktop Items	302
Adjusting the Appearance of Finder Window Contents	303
Managing Internet Preferences	304
Setting Email Preferences	304
Setting Web Browser Preferences	304
Managing Login Preferences	305
Login Window Preferences	305
Deciding How a User Logs In	305
Helping Users Remember Passwords	306
Preventing Restarting or Shutting Down the Computer at Login	306
Login Items Preferences	307
Opening Applications Automatically After a User Logs In	307
Managing Media Access Preferences	308
Media Access Disc Media Preferences	308
Controlling Access to CDs and DVDs	308
Controlling the Use of Recordable Discs	309
Media Access Other Media Preferences	309
Controlling Access to Hard Drives and Disks	309
Ejecting Items Automatically When a User Logs Out	310
Managing Printing Preferences	311
Printer List Preferences	311
Making Printers Available to Users	311
Preventing Users From Modifying the Printer List	312
Restricting Access to Printers Connected to a Computer	312
Printer Access Preferences	313
Setting a Default Printer	313
Restricting Access to Printers	313

7 Print Service 315

- What Printers Can Be Shared? 316
- Who Can Use Shared Printers? 317
- Setup Overview 317
- Before You Begin 319
 - Security Issues 319
- Setting Up Print Service 319
 - Starting Up and Configuring Print Service 319
 - Adding Printers 320
 - Configuring Print Queues 320
 - Adding Print Queues to Shared Open Directory Domains 321
- Setting Up Print Quotas 322
 - Enforcing Quotas for a Print Queue 322
- Setting Up Printing on Client Computers 323
 - Mac OS X Clients 323
 - Adding a Print Queue in Mac OS X Using AppleTalk 323
 - Adding a Print Queue in Mac OS X Using LPR 323
 - Adding a Print Queue From an Open Directory Domain 323
 - Mac OS 8 and Mac OS 9 Clients 324
 - Setting Up Printing on Mac OS 8 or 9 Client for an AppleTalk Printer 324
 - Setting Up Printing on Mac OS 8 or 9 Clients for an LPR Printer 324
- Windows Clients 325
- UNIX Clients 325
- Managing Print Service 325
 - Monitoring Print Service 325
 - Stopping Print Service 326
 - Setting Print Service to Start Automatically 326
- Managing Print Queues 326
 - Monitoring a Print Queue 326
 - Putting a Print Queue on Hold (Stopping a Print Queue) 327
 - Restarting a Print Queue 327
 - Changing a Print Queue's Configuration 327
 - Renaming a Print Queue 328
 - Selecting a Default Print Queue 329

Deleting a Print Queue	329
Managing Print Jobs	329
Monitoring a Print Job	329
Stopping a Print Job	330
Putting a Print Job on Hold	330
Restarting a Print Job	330
Holding All New Print Jobs	331
Setting the Default Priority for New Print Jobs	331
Changing a Print Job's Priority	331
Deleting a Print Job	332
Managing Print Quotas	332
Suspending Quotas for a Print Queue	332
Managing Print Logs	332
Viewing Print Logs	333
Archiving Print Logs	333
Deleting Print Log Archives	334
Solving Problems	334
Print Service Doesn't Start	334
Users Can't Print	334
Print Jobs Don't Print	334
Print Queue Becomes Unavailable	335
8 Web Service	337
Before You Begin	338
Configuring Web Service	338
Providing Secure Transactions	338
Setting Up Web Sites	338
Hosting More Than One Web Site	339
Understanding WebDAV	339
Defining Realms	339
Setting WebDAV Privileges	339
Understanding WebDAV Security	339
Understanding Multipurpose Internet Mail Extension (MIME)	340
Setting Up Web Service for the First Time	341
Managing Web Service	342

Starting or Stopping Web Service	343
Starting Web Service Automatically	343
Modifying MIME Mappings	343
Setting Up Persistent Connections for Web Service	344
Limiting Simultaneous Connections for Web Service	344
Setting Up Proxy Caching for Web Service	345
Blocking Web Sites From Your Web Server Cache	345
Enabling SSL for Web Service	346
Setting Up the SSL Log for a Web Server	346
Setting Up WebDAV for a Web Server	346
Starting Tomcat	347
Checking Web Service Status	348
Viewing Logs of Web Service Activity	348
Setting Up Multiple IP Addresses for a Port	348
Managing Web Sites	349
Setting Up the Documents Folder for Your Web Site	349
Changing the Default Web Folder for a Site	349
Enabling a Web Site on a Server	350
Setting the Default Page for a Web Site	351
Changing the Access Port for a Web Site	351
Improving Performance of Static Web Sites	351
Enabling Access and Error Logs for a Web Site	352
Setting Up Directory Listing for a Web Site	352
Connecting to Your Web Site	353
Enabling WebDAV	353
Setting Access for WebDAV-Enabled Sites	354
Enabling a Common Gateway Interface (CGI) script	354
Enabling Server Side Includes (SSI)	355
Monitoring Web Sites	356
Setting Server Responses to MIME Types	356
Enabling SSL	357
Enabling PHP	357
WebMail	358
WebMail Users	358

WebMail and Your Mail Server	359
WebMail Protocols	359
Enabling WebMail	359
Configuring WebMail	360
Setting Up Secure Sockets Layer (SSL) Service	361
Generating a Certificate Signing Request (CSR) for Your Server	361
Obtaining a Web Site Certificate	362
Installing the Certificate on Your Server	363
Enabling SSL for the Site	363
Solving Problems	364
Users Can't Connect to a Web Site on Your Server	364
A Web Module Is Not Working as Expected	364
A CGI Will Not Run	364
Installing and Viewing Web Modules	365
Macintosh-Specific Modules	365
mod_machinary_apple	365
mod_sherlock_apple	365
mod_auth_apple	365
mod_redirectcgi_apple	366
mod_hfs_apple	366
Open-Source Modules	366
Tomcat	366
PHP: Hypertext Preprocessor	366
mod_perl	366
MySQL	367
Where to Find More Information	367
9 Mail Service	369
Mail Service Protocols	370
Post Office Protocol (POP)	370
Internet Message Access Protocol (IMAP)	371
Simple Mail Transfer Protocol (SMTP)	371
SMTP Alternatives: Sendmail and Postfix	371
How Mail Service Uses SSL	372
How Mail Service Uses DNS	372

Where Mail Is Stored	373
How User Account Settings Affect Mail Service	373
What Mail Service Can Do About Junk Mail	373
SMTP Authentication	374
Restricted SMTP Relay	374
SMTP Authentication and Restricted SMTP Relay Combinations	375
Rejected SMTP Servers	375
Mismatched DNS Name and IP Address	375
Blacklisted Servers	375
What Mail Service Doesn't Do	376
Mail Service Configuration in the Local Directory	376
Overview of Mail Service Tools	376
Setup Overview	377
Overview of Ongoing Mail Service Management	379
Before You Begin	379
Working With General Settings for Mail Service	380
Starting and Stopping Mail Service	380
Starting Mail Service Automatically	380
Requiring or Allowing Kerberos Authentication	381
Adding or Removing Local Names for the Mail Server	381
Changing Protocol Settings for Mail Service	382
Monitoring and Archiving Mail	382
Working With Settings for Incoming Mail	382
Limiting Incoming Message Size	383
Deleting Email Automatically	383
Notifying Users Who Have New Mail	383
Working With Settings for Incoming POP Mail	384
Requiring Authenticated POP (APOP)	384
Changing the POP Response Name	384
Changing the POP Port Number	385
Working With Settings for Incoming IMAP Mail	385
Requiring Secure IMAP Authentication	385
Changing the IMAP Response Name	386
Using Case-Sensitive IMAP Folder Names	386

Controlling IMAP Connections Per User	386
Terminating Idle IMAP Connections	387
Changing the IMAP Port Number	387
Working With Settings for Outgoing Mail	387
Sending Nonlocal Mail	388
Sending Only Local Mail	388
Suspending Outgoing Mail Service	388
Working With Settings for SMTP Mail	389
Requiring SMTP Authentication	389
Sending SMTP Mail via Another Server	389
Changing the SMTP Response Names	390
Changing the Incoming SMTP Port Number	391
Changing the Outgoing SMTP Port Number	391
Enabling an Alternate Mail Transfer Agent	391
Starting Sendmail	392
Working With the Mail Database	393
Converting the Mail Database From an Earlier Version	393
Changing Where Mail Is Stored	394
Configuring Automatic Mail Deletion	394
Allowing Administrator Access to the Mail Database and Files	394
Cleaning Up the Mail Files	395
Working With Network Settings for Mail Service	396
Specifying DNS Lookup for Mail Service	396
Updating the DNS Cache in Mail Service	397
Changing Mail Service Timeouts	397
Limiting Junk Mail	398
Restricting SMTP Relay	398
Rejecting SMTP Connections From Specific Servers	399
Checking for Mismatched SMTP Server Name and IP Address	399
Rejecting Mail From Blacklisted Senders	401
Allowing SMTP Relay for a Backup Mail Server	401
Filtering SMTP Connections	401
Working With Undeliverable Mail	402
Forwarding Undeliverable Incoming Mail	402

Limiting Delivery Attempts in Mail Service	402
Sending Nondelivery Reports to Postmaster	403
Monitoring Mail Status	403
Viewing Overall Mail Service Activity	404
Viewing Connected Mail Users	404
Viewing Mail Accounts	404
Reviewing Mail Service Logs	404
Reclaiming Disk Space Used by Mail Service Logs	405
Supporting Mail Users	405
Configuring Mail Settings for User Accounts	405
Configuring Email Client Software	406
Creating Additional Email Addresses for a User	407
Performance Tuning	407
Backing Up and Restoring Mail Files	408
Where to Find More Information	408
Books	408
Internet	409

10 Client Management: Mac OS 9 and OS 8 411

The User Experience	412
Logging In	412
Logging In Using the All Other Users Account	413
Logging In Using the Guest Account	413
Locating the Home Directory	413
Finding Applications	414
Finding Shared Documents	414
Before You Begin	414
Client Computer Requirements	414
Administrator Computer Requirements	415
Using Update Packages	417
Choosing a Language for Macintosh Manager Servers and Clients	417
Changing the Apple File Service Language Script	418
Inside Macintosh Manager	418
Macintosh Manager Security	418
About the Macintosh Manager Share Point	419

The Multi-User Items Folder	419
How the Multi-User Items Folder Is Updated	420
How Macintosh Manager Works With Directory Services	420
Where User Information Is Stored	421
How Macintosh Manager Works With Home Directories	422
How Macintosh Manager Works With Preferences	422
Where Macintosh Manager Preferences Are Stored	422
Using the MMLocalPrefs Extension	423
Using NetBoot With Macintosh Manager	423
Preparation for Using NetBoot	423
Setting Up Mac OS 9 or Mac OS 8 Managed Clients	424
Logging In to Macintosh Manager as an Administrator	425
Working With Macintosh Manager Preferences	426
Importing User Accounts	426
Applying User Settings With a Template	426
Importing All Users	427
Importing One or More Users	427
Collecting User Information in a Text File	428
Importing a List of Users From a Text File	428
Finding Specific Imported Users	429
Providing Quick Access to Unimported Users	429
Using Guest Accounts	429
Providing Access to Unimported Mac OS X Server Users	430
Setting Up a Guest User Account	431
Designating Administrators	431
About Macintosh Manager Administrators	431
Allowing Mac OS X Server Administrators to Use Macintosh Manager Accounts	432
About Workgroup Administrators	432
Creating a Macintosh Manager Administrator	432
Creating a Workgroup Administrator	432
Changing Your Macintosh Manager Administrator Password	433
Working With User Settings	433
Changing Basic User Settings	433
Allowing Multiple Logins for Users	434

Granting a User System Access	434
Changing Advanced Settings	434
Limiting a User's Disk Storage Space	435
Updating User Information From Mac OS X Server	435
Setting Up Workgroups	436
Types of Workgroup Environments	436
Creating a Workgroup	436
Using a Template to Apply Workgroup Settings	437
Creating Workgroups From an Existing Workgroup	437
Modifying an Existing Workgroup	438
Using Items Settings	438
Setting Up Shortcuts to Items for Finder Workgroups	438
Making Items Available to Panels or Restricted Finder Workgroups	439
Making Items Available to Individual Users	440
Using Privileges Settings	440
Protecting the System Folder and Applications Folder	440
Protecting the User's Desktop	440
Preventing Applications From Altering Files	441
Preventing Access to FireWire Disks	441
Allowing Users to Play Audio CDs	441
Allowing Users to Take Screen Shots	442
Allowing Users to Open Applications From a Disk	442
Setting Access Privileges for Removable Media	442
Setting Access Privileges for Menu Items	443
Sharing Information in Macintosh Manager	443
Selecting Privileges for Workgroup Folders	444
Setting Up a Shared Workgroup Folder	444
Setting Up a Hand-In Folder	445
Using Volumes Settings	445
Connecting to AFP Servers	445
Providing Access to Server Volumes	446
Using Printers Settings	447
Making Printers Available to Workgroups	447
Setting a Default Printer	447

Restricting Access to Printers	448
Setting Print Quotas	448
Allowing Users to Exceed Print Quotas	448
Setting Up a System Access Printer	449
Using Options Settings	449
Choosing a Location for Storing Group Documents	450
Making Items Open at Startup	450
Checking for Email When Users Log In	451
Creating Login Messages for Workgroups	451
Setting Up Computer Lists	451
Creating Computer Lists	451
Setting Up the All Other Computers Account	452
Duplicating a Computer List	452
Creating a Computer List Template	453
Disabling Login for Computers	453
Using Workgroup Settings for Computers	454
Controlling Access to Computers	454
Using Control Settings	454
Disconnecting Computers Automatically to Minimize Network Traffic	454
Setting the Computer Clock Using the Server Clock	455
Using a Specific Hard Disk Name	455
Creating Email Addresses for Managed Users	455
Using Security Settings for Computers	456
Keeping Computers Secure If a User Forgets to Log Out	456
Allowing Access to All CDs and DVDs	457
Allowing Access to Specific CDs or DVDs	457
Choosing Computer Security Settings for Applications	457
Allowing Specific Applications to Be Opened by Other Applications	458
Allowing Users to Work Offline	458
Allowing Users to Switch Servers After Logging In	459
Allowing Users to Force-Quit Applications	459
Allowing Users to Disable Extensions	459
Using Computer Login Settings	460
Choosing How Users Log In	460

Creating Login Messages for Computers	460
Customizing Panel Names	460
Managing Portable Computers	461
Portable Computers With Network Users	461
Portable Computers With Local Users	461
Letting Users Check Out Computers	462
Using Wireless Services	462
Using Global Security Settings	462
Using Macintosh Manager Reports	463
Setting the Number of Items in a Report	463
Keeping the Administration Program Secure	463
Verifying Login Information Using Kerberos	464
Preventing Users From Changing Their Passwords	464
Allowing Administrators to Access User Accounts	464
Copying Preferences for Mac OS 8 Computers	464
Using Global CD-ROM Settings	465
Managing Preferences	466
Using Initial Preferences	466
Using Forced Preferences	467
Preserved Preferences	468
Solving Problems	470
I've Forgotten My Administrator Password	470
Administrators Can't Get to the Finder After Logging In	470
Generic Icons Appear in the Items Pane	470
Selecting "Local User" in the Multiple Users Control Panel Doesn't Work	471
Some Printers Don't Appear in the Available Printers List	471
Users Can't Log In to the Macintosh Manager Server	471
Users Can't Log In as "Guest" on Japanese-Language Computers	471
A Client Computer Can't Connect to the Server	471
The Server Doesn't Appear in the AppleTalk List	472
The User's Computer Freezes	472
Users Can't Access Their Home Directories	472
Users Can't Access Shared Files	472
Shared Workgroup Documents Don't Appear in a Panels Environment	472

Applications Don't Work Properly or Don't Open	472
Users Can't Drag and Drop Between Applications	473
Users Can't Open Files From a Web Page	473
Sometimes the Right Application Doesn't Open for Users	473
Where to Find More Information	473

11 DHCP Service 475

Before You Set Up DHCP Service	475
Creating Subnets	476
Assigning IP Addresses Dynamically	476
Using Static IP Addresses	476
Locating the DHCP Server	476
Interacting With Other DHCP Servers	477
Assigning Reserved IP Addresses	477
Setting Up DHCP Service for the First Time	477
Managing DHCP Service	478
Starting and Stopping DHCP Service	478
Setting the Default DNS Server for DHCP Clients	479
Setting the LDAP Server for DHCP Clients	479
Setting Up Logs for DHCP Service	480
Deleting Subnets From DHCP Service	480
Changing Lease Times for Subnet Address Ranges	480
Monitoring DHCP Client Computers	481
Creating Subnets in DHCP Service	481
Changing Subnet Settings in DHCP Service	481
Setting DNS Options for a Subnet	482
Setting NetInfo Options for a Subnet	482
Disabling Subnets Temporarily	483
Viewing DHCP and NetBoot Client Lists	483
Viewing DHCP Log Entries	483
Solving Problems	484
Where to Find More Information	484

12 NetBoot 485

Prerequisites	486
---------------	-----

Administrator Requirements	486
Server Requirements	486
Client Computer Requirements	487
Network Requirements	488
Capacity Planning	488
NetBoot Implementation	489
NetBoot Image Folder	489
Property List File	490
Boot Server Discovery Protocol (BDSP)	491
TFTP and the Boot ROM File	492
NetBoot Files and Directory Structure	493
Security	493
NetBoot and AirPort	493
Setup Overview	493
Setting Up NetBoot on a Mac OS X Server	496
Creating a Mac OS X Disk Image	496
Installing Classic (Mac OS 9) on a Mac OS X Disk Image	497
Installing the Mac OS 9 Disk Image	497
Modifying the Mac OS 9 Disk Image	498
Specifying the Default NetBoot Disk Image	500
Setting Up Multiple Disk Images	500
Configuring NetBoot on Your Server	501
Starting NetBoot on Your Server	501
Enabling NetBoot Disk Images	502
Managing NetBoot	502
Turning Off NetBoot	502
Disabling Disk Images	502
Updating Mac OS X Disk Images	503
Monitoring the Status of Mac OS X NetBoot Clients	503
Monitoring the Status of Mac OS 9 NetBoot Clients	503
Filtering NetBoot Client Connections	503
Load Balancing	504
Enabling Server Selection	504
Using Share Points to Spread the Load	505

Supporting Client Computers	505
Updating the Startup Disk Control Panel	505
Setting Up “System-Less” Clients	506
Selecting a NetBoot Startup Image (from Mac OS X)	506
Selecting a NetBoot Startup Image (from Mac OS 9)	506
Starting Up Using the N Key	507
Solving Problems	507
A NetBoot Client Computer Won’t Start Up	507
You Are Using Macintosh Manager and a User Can’t Log In to a NetBoot Client	508

13 Network Install 509

Understanding Packages	509
Setup Overview	510
Setting Up Network Install	511
Creating a Network Install Disk Image	511
Creating Custom Packages for Network Install	512
Including Packages in an Installer Disk Image	512
Enabling Installer Disk Images	513

14 DNS Service 515

Before You Set Up DNS Service	516
DNS and BIND	516
Setting Up Multiple Name Servers	516
Using DNS With Mail Service	516
Setting Up DNS Service for the First Time	517
Managing DNS Service	518
Starting and Stopping DNS Service	518
Viewing DNS Log Entries	519
Viewing DNS Service Status	519
Viewing DNS Usage Statistics	519
Inside DNS Service (Configuring BIND)	520
What Is BIND?	520
BIND on Mac OS X Server	520
BIND Configuration File	520
Zone Data Files	521

Practical Example	521
Setting Up Sample Configuration Files	521
Configuring Clients	522
Check Your Configuration	523
Load Distribution With Round Robin	523
Setting Up a Private TCP/IP Network	523
Where to Find More Information	524
15 Firewall Service	525
Before You Set Up Firewall Service	527
What Is a Filter?	527
IP Address	527
Subnet Mask	527
Using Address Ranges	528
IP Address Precedence	529
Multiple IP Addresses	529
Practical Examples	529
Block Access to Internet Users	529
Block Junk Mail	530
Allow a Customer to Access the Apple File Server	530
Setting Up Firewall Service for the First Time	530
Managing Firewall Service	531
Starting and Stopping Firewall Service	531
Setting Firewall Service to Start Automatically	531
Editing IP Filters	532
Creating an IP Filter	532
Searching for IP Filters	533
Viewing the Firewall Log	533
Configuring Firewall Service	533
Setting Up Logs for Firewall Service	534
Viewing Denied Packets	535
Filtering UDP Ports in Firewall Service	535
Blocking Multicast Services in Firewall Service	536
Allowing NetInfo Access to Certain IP Addresses	536
Changing the Any Port (Default) Filter	537

	Preventing Denial-of-Service Attacks	537
	Creating IP Filter Rules Using ipfw	538
	Reviewing IP Filter Rules	539
	Creating IP Filter Rules	539
	Deleting IP Filter Rules	539
	Port Reference	540
	Solving Problems	543
	You Can't Access the Server Over TCP/IP	543
	You Can't Locate a Specific Filter	543
	Where to Find More Information	543
16	SLP DA Service	545
	SLP DA Considerations	545
	Before You Begin	545
	Managing Service Location Protocol (SLP) Directory Agent (DA) Service	547
	Starting and Stopping SLP DA Service	547
	Viewing Scopes and Registered Services in SLP	547
	Creating New Scopes in SLP DA Service	548
	Registering a Service With SLP DA	548
	Deregistering Services in SLP DA Service	549
	Setting Up Logs for SLP DA Service	549
	Logging Debugging Messages in SLP DA Service	549
	Viewing SLP DA Log Entries	549
	Using the Attributes List	550
	Where to Find More Information	550
17	Tools for Advanced Users	551
	Terminal	552
	Using the Terminal Application	552
	Understanding UNIX Command-Line Structure	553
	Secure Shell (SSH) Command	553
	Enabling and Disabling SSH Access	553
	Opening an SSH Session	553
	Executing Commands in an SSH Session	554
	Closing an SSH Session	554

Understanding Key Fingerprints	554
dsimportexport	555
Log Rolling Scripts	555
diskspacemonitor	556
diskutil	557
installer	558
Using installer	558
Full Operating System Installation	559
softwareupdate	561
systemsetup	561
Working With Server Identity and Startup	561
Working With Date and Time Preferences	562
Working With Sleep Preferences	562
networksetup	562
Reverting to Previous Network Settings	563
Retrieving Your Server's Network Configuration	563
Configuring TCP/IP Settings	564
Configuring DNS Servers and Search Domains	564
Managing Network Services	564
Designating Proxy Servers	565
MySQL Manager	565
Simple Network Management Protocol (SNMP) Tools	566
diskKeyFinder	566
Enabling IP Failover	567
Requirements	567
Hardware	567
Software	567
Failover Operation	567
Enabling IP Failover	569
Configuring IP Failover	569
Notification Only	570
Pre And Post Scripts	570

Appendix A
Open Directory Data Requirements 573

User Data That Mac OS X Server Uses 573

Standard Data Types in User Records 574

Format of the MailAttribute Data Type 577

Standard Data Types in Group Records 580

Glossary 581

Index 591

How to Use This Guide

What's Included in This Guide

This guide consists primarily of chapters that tell you how to administer individual Mac OS X Server services:

- Chapter 1, “Administering Your Server,” highlights the major characteristics of Mac OS X Server’s services and takes you on a tour of its administration applications.
- Chapter 2, “Directory Services,” describes the services that Mac OS X computers use to find information about users, groups, and devices on your network. The Mac OS X directory services architecture is referred to as *Open Directory*.
- Chapter 3, “Users and Groups,” covers user and group accounts, describing how to administer settings for server users and collections of users (groups), including Open Directory Password Server and other password authentication options.
- Chapter 4, “Sharing,” tells you how to share folders, hard disks, and CDs among network users, as well as how to make them automatically visible after logging in to Mac OS X computers.
- 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, “Client Management: Mac OS X,” addresses client management for Mac OS X computer users. Client management lets you customize a user’s working environment and restrict a user’s access to network resources.
- Chapter 7, “Print Service,” tells you how to share printers among users on Macintosh, Windows, and other computers.
- Chapter 8, “Web Service,” describes how to set up and administer a Web server and host multiple Web sites on your server.
- Chapter 9, “Mail Service,” describes how to set up and administer a mail server on your server.

- Chapter 10, “Client Management: Mac OS 9 and OS 8,” addresses client management for Mac OS 8 and 9 computer users, describing how to use Macintosh Manager to manage their day-to-day working environments.
- Chapter 11, “DHCP Service,” describes Dynamic Host Configuration Protocol (DHCP) service, which lets you dynamically allocate IP addresses to the computers used by server users.
- Chapter 12, “NetBoot,” describes the application that lets Macintosh Mac OS 9 and X computers boot from a network-based system image.
- Chapter 13, “Network Install,” tells you how to use the centralized network software installation service that automates installing, restoring, and upgrading Macintosh computers on your network.
- Chapter 14, “DNS Service,” describes Dynamic Name Service (DNS), a distributed database that maps IP addresses to domain names.
- Chapter 15, “Firewall Service,” addresses how to protect your server by scanning incoming IP packets and rejecting or accepting these packets based on filters you create.
- Chapter 16, “SLP DA Service,” describes Service Location Protocol Directory Assistant (SLP DA), which you can use to make devices on your network visible to your server users.
- Chapter 17, “Tools for Advanced Users,” describes server applications, tools, and techniques intended for use by experienced server administrators.
- Appendix A, “Open Directory Data Requirements,” provides information you’ll need when you must map directory services information needed by Mac OS X to information your server will retrieve from another vendor’s server.
- The Glossary defines terms you’ll encounter as you read this guide.

Using This Guide

Review the first chapter to acquaint yourself with the services and applications that Mac OS X Server provides.

Then 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, how to set it up for the first time, and how to administer it over time.

Also take a look at any chapter that describes a service 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.

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

Setting Up Mac OS X Server for the First Time

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

- Refer to *Getting Started With Mac OS X Server*, the document that came with your software, for instructions on server installation and setup. For many environments, this document provides all the information you need to get your server up, running, and available for initial use.
- Review Chapter 1, “Administering Your Server,” in this guide to determine which services you'd like to refine and expand, to identify new services you'd like to set up, and to learn about the server applications you'll use during these activities.
- Read specific chapters to learn how to continue setting up individual services. Pay particular attention to the information in these sections: “Setup Overview,” “Before You Begin,” and “Setting Up 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 day-to-day administration task, you can find step-by-step procedures by using the online help available with server administration programs. While all the administration tasks are also documented in this guide, sometimes it's more convenient to retrieve information in online help form while using your server.

Getting Additional Information

In addition to this document, you'll find information about Mac OS X Server

- in *Getting Started With Mac OS X Server*, which tells you how to install and set up your server initially
- in *Upgrading to Mac OS X Server*, which provides instructions for migrating data to Mac OS X Server from existing Macintosh computers
- at www.apple.com/macosx/server
- in online help on your server
- in Read Me files on your server CD

Administering Your Server

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

- You can connect users to each other, using services such as mail and file sharing.
- You can share system resources, such as printers and computers—maximizing their availability as users move about and making sure that disk space and printer usage remain equitably shared.
- You can host Internet services, such as Web sites and streaming video.
- You can customize working environments—such as desktop resources and personal files—of networked users.

This chapter is a tour of Mac OS X Server capabilities and administration. The chapter begins by pointing out some of Mac OS X Server's key features. Then it summarizes the services you can set up to support the clients you want your server to host. Finally, it introduces the applications you use to set up and administer your server.

Highlighting Key Features

Mac OS X Server has a wide range of features that characterize it as easy to use, yet robust and high performing.

Ease of Setup and Administration

From the time you first unpack your server throughout its initial setup and deployment, its ease of use is prominent.

Setup assistants quickly walk you through the process of making basic services initially available. While your network users take advantage of the initial file sharing, mail, Web and other services, you can add on additional client support and manage day-to-day server operations using graphical administrative applications. From one administrator computer, you can set up and manage all the Mac OS X Servers on your network.

Networking and Security

You can choose from several user authentication options, ranging from Kerberos or Lightweight Directory Access Protocol (LDAP) to Mac OS X Server's Open Directory Password Server.

Password Server lets you implement password policies and supports a wide variety of client protocols. The Password Server is based on a standard known as SASL (Simple Authentication and Security Layer), so it can support a wide range of network user authentication protocols that are used by clients of Mac OS X Server services, such as mail and file servers, that need to authenticate users.

Kerberos authentication is available for file services—Apple Filing Protocol (AFP) and File Transfer Protocol (FTP)—as well as for mail services (POP, IMAP, and SMTP).

External network communication requests can be controlled with built-in Internet Protocol (IP) firewall management. And data communications can be encrypted and authenticated with protocol-level data security provided with Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell (SSH).

File and Printer Sharing

File sharing offers flexible support for various native protocols as well as security and high availability:

- It's easy to share files with Macintosh, Windows, UNIX, Linux, and anonymous Internet clients.
- You can control how much file space individual users consume by setting up mail and file quotas. Quotas limit the number of megabytes a user can use for mail or files.
- Kerberos authentication is available for AFP and FTP file servers.
- You can improve the security of NFS volumes by setting up share points on them that let users access them using the more secure AFP protocol. This feature is referred to as *resharing NFS mounts*.
- AFP autoreconnect lets client computers keep Apple file servers mounted after long periods of inactivity or after sleep/wake cycles.

Mac OS X Server printer sharing includes

- the ability to set up print quotas. Print quotas can be set up for each user and each print queue, letting you limit the number of pages that can be printed during a particular period.
- support for sharing printers among Mac OS 9 users (AppleTalk and LaserWriter 8 support), Mac OS X, Windows, and UNIX users

Open Directory Services

User and group information is used by your server to authenticate users and authorize their access to services and files. Information about other network resources is used by your server to make printers and other devices available to particular users. To access this information, the server retrieves it from centralized data repositories known as *directory domains*. The term for the services that locate and retrieve this data is *directory services*.

The Mac OS X directory services architecture is referred to as *Open Directory*. It lets you store data in a way that best suits your environment. Mac OS X Server can host directory domains using Apple's NetInfo and LDAP directory domains. Open Directory also lets you take advantage of information you have already set up in non-Apple directory domains—for example, LDAP or Active Directory servers or Berkeley Software Distribution (BSD) configuration files.

Comprehensive Management of Macintosh Workgroups

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

Mac OS X Server client management support helps you personalize the computing environment of Macintosh clients. You can set up Mac OS 8, 9, and X computers to have particular desktop environments and access to particular applications and network resources. You can design your Macintosh users' experience as circumstances warrant.

You can also use NetBoot and Network Install to automate the setup of software used by Macintosh client computers:

- NetBoot lets Macintosh Mac OS 9 and X computers boot from a network-based system image, offering quick and easy configuration of department, classroom, and individual systems as well as Web and application servers throughout a network. When you update NetBoot images, all NetBooted computers have instant access to the new configuration.
- Network Install is a centralized network software installation service. It lets you selectively and automatically install, restore, or upgrade network-based Macintosh systems anywhere in the organization.

Mac OS X Server also lets you automatically configure the directory services you want Mac OS X clients to have access to. Automatic directory services configuration means that when a user logs into a Mac OS X computer, the user's directory service configuration is automatically downloaded from the network, setting up the user's network access policies, preferences, and desktop configuration without the need to configure the client computer directly.

High Availability

To maximize server availability, Mac OS X Server includes technology for monitoring server activity, monitoring and reclaiming disk space, automatically restarting malfunctioning services, and automatically restarting the server following a power failure.

You can also configure *IP failover*. IP failover is a way to set up a standby server that will take over if the primary server fails. The standby server takes over the IP address of the failed server, which takes the IP address back when it is online again. IP failover is useful for DNS servers, Web servers hosting Web sites, media broadcast servers, and other servers that require minimal data replication.

Extensive Internet and Web Services

Powerful Internet and Web services are built into Mac OS X Server:

- Apache, the most popular Web server, provides reliable, high-performance Web content delivery. Integrated into Apache is Web-Based Distributed Authoring and Versioning (WebDAV), which simplifies the Web publishing and content management environment.
- If your Web sites contain static HTML files that are frequently requested, you can enable a performance cache to improve server performance.
- Web services include a comprehensive assortment of open-source services—Ruby, Tomcat, MySQL, PHP, and Perl.
- Mac OS X Server includes a high-performance Java virtual machine.
- SSL support enables secure encryption and authentication for ecommerce Web sites and confidential materials.
- QuickTime Streaming Server (QTSS) lets you stream both live and stored multimedia content on the Internet using industry-standard protocols.
- Mail service lets you set up a mail server your network users can use to send and receive email.
- WebMail service bundled with Mac OS X Server enables your users to access mail service via a Web browser.

Highlighting Individual Services

This section highlights individual Mac OS X Server services and tells you where in this guide to find more information about them.

Directory Services

Directory services let you use a central data repository for user and network information your server needs to authenticate users and give them access to services. Information about users (such as their names, passwords, and preferences) as well as printers and other resources on the network is consolidated rather than distributed to each computer on the network, simplifying the administrator's tasks of directory domain setup and maintenance.

Open Directory

On Mac OS X computers, the directory services are collectively referred to as Open Directory. Open Directory acts as an intermediary between directory domains that store information and Mac OS X processes that need the information.

Open Directory supports a wide variety of directory domains, letting you store your directory information on Mac OS X Server or on a server you already have set up for this purpose:

- You can define and manage information in directory domains that reside on Mac OS X Server. Open Directory supports both NetInfo and LDAPv3 protocols and gives you complete control over directory data creation and management.
- Mac OS X Server can also retrieve directory data from LDAP and Active Directory servers and BSD configuration files you've already set up. Your server provides full read/write and SSL communications support for LDAPv3 directory domains.

Chapter 2, "Directory Services," provides complete information about all the Open Directory options, including instructions for how to create Mac OS X–resident directory domains and how to configure your server and your clients to access directory domains of all kinds.

Chapter 3, "Users and Groups," describes how to work with user and group accounts stored in Open Directory domains.

Password Validation

Open Directory gives you several options for validating a user's password:

- Using a value stored as a readable attribute in the user's account.
- Using a value stored in the Open Directory Password Server. This strategy lets you set up user-specific password policies for users. For example, you can require a user to change his password periodically or use only passwords having more than a minimum number of characters.

Password Server supports a wide range of client authentication protocols.

- Using a Kerberos server.
- Using LDAP bind authentication with a non-Apple LDAPv3 directory server.

"Understanding Password Validation" on page 189 provides more information about these options and tells you how to implement them.

Search Policies

Before a user can log in to or connect with a Mac OS X client or server, he or she must enter a name and password associated with a user account that the computer can find. A Mac OS X computer can find user accounts that reside in a directory domain of the computer's search policy. A *search policy* is a list of directory domains the computer searches when it needs configuration information.

You can configure the search policy of Mac OS X computers on the computers themselves. You can automate Mac OS X client directory setup by using your server's built-in DHCP Option 95 support.

Chapter 2, "Directory Services," describes how to configure search policies on any Mac OS X computer.

File Services

Mac OS X Server makes it easy to share files using the native protocols of different kinds of client computers. 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, and to provide name resolution service for Windows clients.
- File Transfer Protocol (FTP) service lets you share files with anyone using FTP.
- Network File System (NFS) service lets you share files and folders with users who have NFS client software (UNIX users).

You can deploy network home directories for Mac OS X clients using AFP and for UNIX clients using NFS. With a network home directory, users can access their applications, documents, and individual settings regardless of the computer to which they log in. You can impose disk quotas on network home directories to regulate server disk usage for users with home directories.

Sharing

You share files among users by designating share points. A *share point* is a folder, hard disk (or hard disk partition), or CD that you make accessible over the network. It's the point of access at the top level of a group of shared items.

On Mac OS X computers, share points can be found in the /Network directory and by using the Finder's Connect To Server command. On Mac OS 8 and 9 computers, users access share points using the Chooser. On Windows computers, users use Network Neighborhood. Chapter 4, "Sharing," tells you how to set up and manage share points.

Static file server listings can also be published in a non-Apple directory domain, making it easy for computers in your company that are not on your local network to discover and connect to Mac OS X Server.

Apple File Service

Apple Filing Protocol (AFP) 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.

AFP offers

- file sharing support for Macintosh clients over TCP/IP
- autoreconnect support when a file server connection is interrupted
- encrypted file sharing (AFP through SSH)
- automatic creation of user home directories
- Kerberos v5 authentication for Mac OS X v10.2 and later clients
- fine-grain access controls for managing client connections and guest access
- automatic disconnect of idle clients after a period of inactivity

AFP also lets you reshare NFS mounts using AFP. This feature provides a way for clients not on the local network to access NFS volumes via a secure, authenticated AFP connection. It also lets Mac OS 9 clients access NFS file services on traditional UNIX networks.

See “Apple File Service” on page 224 for details about AFP.

Windows Services

Windows services in Mac OS X Server provide four native services to Windows clients:

- file service, which allows Windows clients to connect to Mac OS X Server using Server Message Block (SMB) protocol over TCP/IP
- print service, which 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

See “Windows Services” on page 235 for more information about Windows services.

Network File System (NFS) Service

NFS is the protocol used for file services on UNIX computers.

The NFS term for sharing is *export*. You can export a shared item to a set of client computers or to “World.” Exporting an NFS volume to World means that anyone who can access your server can also access that volume.

NFS does not support name/password authentication. It relies on client IP addresses to authenticate users and on client enforcement of privileges—not a secure approach in most networks. Therefore use NFS only 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.

See “Network File System (NFS) Service” on page 256 for more information about NFS.

File Transfer Protocol (FTP)

FTP allows computers to transfer files over the Internet. Clients using any operating system that supports FTP can connect to your FTP 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.

FTP service in Mac OS X Server supports Kerberos v5 authentication and, for most FTP clients, resuming of interrupted FTP file transfers. Mac OS X Server also supports dynamic file conversion, allowing users to request compressed or decompressed versions of information on the server.

FTP is considered to be an insecure protocol, since user names and passwords are distributed across the Internet in clear text. Because of the security issues associated with FTP authentication, most FTP servers are used as Internet file distribution servers for anonymous FTP users.

Mac OS X Server supports anonymous FTP and by default prevents anonymous FTP users from deleting files, renaming files, overwriting files, and changing file permissions. Explicit action must be taken by the server administrator to allow uploads from anonymous FTP users, and then only into a specific share point.

See “File Transfer Protocol (FTP) Service” on page 244 for details about FTP.

Print Service

Print service in Mac OS X Server lets you share network and direct-connect printers among clients on your network. Print service also includes support for managing print queues, monitoring print jobs, logging, and using print quotas.

Print service lets you

- share printers with Mac OS 9 (PAP, LaserWriter 8), Mac OS X (IPP, LPR/LPD), Windows (SMB/CIFS), and UNIX (LPR/LPD) clients
- share direct-connect USB printers with Mac OS X version 10.2 and later clients
- connect to network printers using AppleTalk, LPR, and IPP and connect to direct-connect printers using USB
- make printers visible using Open Directory directory domains

- impose print quotas to limit printer usage

See Chapter 7, “Print Service,” for information about print service.

Web Service

Web service in Mac OS X Server is based on Apache, an open-source HTTP Web server. A Web server responds to requests for HTML Web pages stored on your site. Open-source software allows anyone to view and modify the source code to make changes and improvements. This has led to Apache’s widespread use, making it the most popular Web server on the Internet today.

Web service 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, (WebDAV). With WebDAV capability, your client users can check out Web pages, make changes, and then check the pages back in while the site is running. In addition, Mac OS X users can use a WebDAV-enabled Web server as if it were a file server.

Web service’s Secure Sockets Layer (SSL) support enables secure encryption and authentication for ecommerce Web sites and confidential materials. An easy-to-use digital certificate provides non-forgable proof of your Web site identity.

Mac OS X Server offers extensive support for dynamic Web sites:

- Web service supports Java Servlets, JavaServer Pages, MySQL, PHP, Perl, and UNIX and Mac CGI scripts.
- Mac OS X Server also includes WebObjects deployment software. 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. You can also purchase the WebObjects development tools if you want to create WebObjects applications. For more information and documentation on WebObjects, go to the WebObjects Web page:

www.apple.com/webobjects

See Chapter 8, “Web Service,” for details about Web service.

Mail Service

Mail services support the SMTP, POP, and IMAP protocols, allowing you to select a local or server-based mail storage solution for your users.

With remote mail administration you can manage the message database from any IMAP client. Realtime Blackhole List support allows you to block messages from known spam sources. Support for single or dual IMAP/POP3 mail inboxes gives flexibility in mail retrieval; a user can have a POP mailbox for office use and an IMAP mailbox for mobile use. Automatic blind copying (BCC) on incoming mail from specified hosts lets you track email coming from specific sites. You can limit the amount of disk space a user consumes for mail messages.

To protect email communication from eavesdroppers, mail service features SSL encryption of IMAP connections between the mail server and clients, SMTP AUTH authentication using LOGIN and PLAIN, and APOP and Kerberos v5 authentication for POP, IMAP, and SMTP clients.

For complete information about mail services, see Chapter 9, “Mail Service.”

Macintosh Workgroup Management

Mac OS X Server provides work environment personalization for Mac OS 8, 9, and X computer users, ranging from preference management to operating system and application installation automation.

Client Management

You can use Mac OS X Server to manage the work environments of Mac OS 8, 9, and X clients. Preferences you define for individual users, groups of users, and computers provide your Macintosh users with a consistent desktop, application, and network appearance regardless of the Macintosh computer to which they log in.

To manage Mac OS 8 and 9 clients, you use Macintosh Manager, described in Chapter 10, “Client Management: Mac OS 9 and OS 8.” To manage Mac OS X clients, you use Workgroup Manager, as Chapter 6, “Client Management: Mac OS X,” describes.

Mac OS X client management has several advantages:

- You can take advantage of the directory services autoconfiguration capability to automatically set up the directory services used by Mac OS X client computers.
- When you update user, group, and computer accounts, managed Mac OS X users inherit changes automatically. You update Mac OS 8 and 9 accounts independently, using Macintosh Manager.
- You have more direct control over individual system preferences.
- Network home directories and group directories can be mounted automatically at login.

NetBoot

NetBoot lets Macintosh clients boot from a system image located on Mac OS X Server instead of from the client computer’s disk drive. You can set up multiple NetBoot disk images, so you can boot clients into Mac OS 9 or X or even set up customized Macintosh environments for different groups of clients.

NetBoot can simplify the administration and reduce the support normally associated with large-scale deployments of network-based Macintosh systems. NetBoot is ideal for an organization with a number of client computers that need to be identically configured. For example, NetBoot can be a powerful solution for a data center that needs multiple identically configured Web and application servers.

NetBoot allows administrators to configure and update client computers instantly by simply updating a boot image stored on the server. Each image contains the operating system and application folders for all clients on the server. Any changes made on the server are automatically reflected on the clients when they reboot. Systems that are compromised or otherwise altered can be instantly restored simply by rebooting.

See Chapter 12, “NetBoot,” for information about setting up and managing NetBoot.

Network Install

Network Install is a centrally managed installation service that allows administrators to selectively install, restore, or upgrade client computers. Installation images can contain the latest release of Mac OS X, a software update, site-licensed or custom applications, even configuration scripts:

- Network Install is an excellent solution for operating system migrations, installing software updates and custom software packages, restoring computer classrooms and labs, and reimaging desktop and portable computers.
- You can define custom installation images for various departments in an organization, such as marketing, engineering, and sales.

With Network Install you don't need to insert multiple CDs to configure a system. All the installation files and packages reside on the server and are installed onto the client computer at one time. Network Install also includes pre- and post-installation scripts you can use to invoke actions prior to or after the installation of a software package or system image.

See Chapter 13, “Network Install,” for more information about Network Install.

Network Services

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

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- IP firewall
- Service Location Protocol Directory Agent (SLP DA)

DHCP

DHCP 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.

As you learned in “Search Policies” on page 48, you can automate the directory services setup of Mac OS X clients using your DHCP server’s Option 95 support. This option lets client computers learn about their directory settings from an LDAP server.

Chapter 11, “DHCP Service,” provides information about your server’s DHCP capabilities.

DNS

DNS service lets users connect to a network resource, such as a Web or file server, by specifying a host 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 Internet service provider (ISP) who handles DNS for your network, you can set up a DNS server on your Mac OS X Server.

You’ll find complete information about DNS in Chapter 14, “DNS Service.”

IP Firewall

IP firewall 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.

See Chapter 15, “Firewall Service,” for more information about this service.

SLP DA

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, the service 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.

See Chapter 16, “SLP DA Service,” for information about this service.

QuickTime Streaming Service

QuickTime Streaming Server (QTSS) lets you stream multimedia in real time using the industry-standard RTSP/RTP protocols. QTSS supports MPEG-4, MP3, and QuickTime file formats.

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.

For more information about QTSS, refer to the QuickTime Web site:

www.apple.com/quicktime/products/qtss/

You can use QuickTime Broadcaster in conjunction with QTSS when you want to produce a live event. QuickTime Broadcaster allows you to stream live audio and video over the Internet. QuickTime Broadcaster meets the needs of both beginners and professionals by providing preset broadcast settings and the ability to create custom settings. Built on top of the QuickTime architecture, QuickTime Broadcaster enables you to produce a live event using most codecs that QuickTime supports.

When teamed with QuickTime Streaming Server or Darwin Streaming Server, QuickTime Broadcaster can produce a live event for delivery to an audience of any size, from an individual to a large global audience.

For information about QuickTime Broadcaster, go to this Web site and navigate to the QuickTime Broadcaster page:

www.apple.com/quicktime/

Highlighting Server Applications

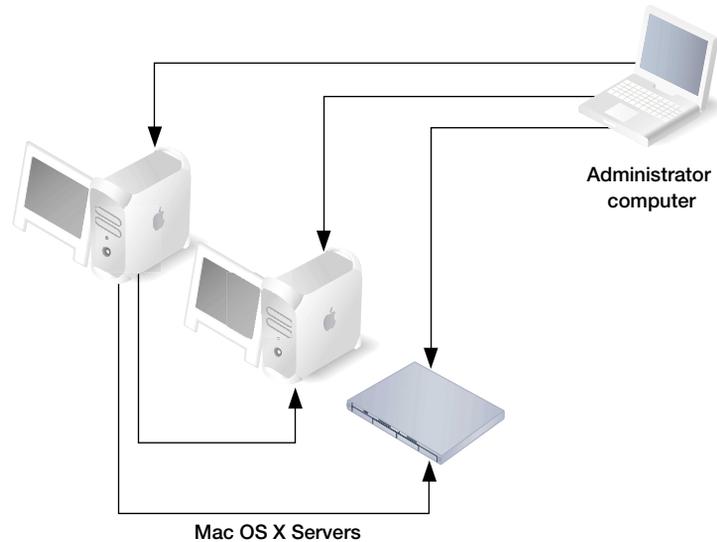
This section introduces you to the applications, tools, and techniques you use to set up and administer your Mac OS X Server. The following table summarizes them and tells you where to find more information about them.

Application, tool, or technique	Use to	For more information, see
Server Assistant	Initialize services	page 58
Open Directory Assistant	Create or set up access to existing NetInfo and LDAPv3 directory domains and create and configure Password Servers	page 58
Directory Access	Configure access to data in existing directory domains and define a search policy	page 59
Workgroup Manager	Administer accounts, manage share points, and administer client management for Mac OS X users	page 59
Server Settings	Configure file, print, mail, Web, NetBoot, and network services	page 60
Server Status	Monitor services	page 61
Macintosh Manager	Administer client management for Mac OS 8 and 9 users	page 62
NetBoot administration tools	Manage NetBoot disk images	page 62
Package Maker	Create Network Install installation packages	page 62
Server Monitor	Review information about Xserve hardware	page 62
Streaming Server Admin	Set up and manage QuickTime Streaming Server (QTSS)	page 63
Terminal	Run command-line tools	page 552
Secure shell (SSH)	Use Terminal to run command-line tools for remote servers securely	page 553
dsimportexport	Import and export user and group accounts using XML or text files	page 555

Application, tool, or technique	Use to	For more information, see
log rolling scripts	Periodically roll, compress, and delete server log files	page 555
diskspacemonitor	Monitor percentage-full disk thresholds and execute scripts that generate email alerts and reclaim disk space when thresholds are reached	page 556
diskutil	Manage Mac OS X Server disks and volumes remotely	page 557
installer	Install software packages remotely	page 558
softwareupdate	Find new versions of software and install them remotely on a server	page 561
systemsetup	Configure system preferences on a remote server	page 561
networksetup	Configure network services for a particular network hardware port on a remote server	page 562
MySQL Manager	Manage the version of MySQL that is installed with Mac OS X Server	page 565
Simple Network Management Protocol (SNMP) administration tools	Monitor your server using the SNMP interface	page 566
diskKeyFinder	Verify the physical location of a remote headless server volume that you want to manage	page 566
Enabling IP failover	Set up a standby server that takes over if the primary server fails	page 567

Administering a Server From Different Computers

You can use the server applications to manage the local server or to manage a remote server, including headless servers. You can also manage Mac OS X Servers remotely from an administrator computer. An *administrator computer* is a Mac OS X computer onto which you have installed the server applications from the Mac OS X Server Administration Tools CD.



The following sections give you more information about the first 11 applications in the table above, including instructions for using them to manage a remote server. The remaining applications and tools are for use by experienced server administrators; see Chapter 17, “Tools for Advanced Users,” for information about them.

Server Assistant

Server Assistant is the application you use to perform initial service setup of a Mac OS X Server. You can use Server Assistant the first time you set up a local or remote Mac OS X Server. See *Getting Started With Mac OS X Server* for instructions.

Open Directory Assistant

Use Open Directory Assistant to create shared server–resident NetInfo or LDAPv3 directory domains, set up Password Servers, and configure access to shared domains and Password Servers.

You can run Open Directory Assistant immediately after running Server Assistant, or you can run it later, as many times as you like.

You'll find Open Directory Assistant in /Applications/Utilities/. For information about how to use the application, see Chapter 2, "Directory Services."

Directory Access

Directory Access is the primary application for setting up a Mac OS X computer's connections with directory domains as well as defining the computer's search path.

Unlike Open Directory Assistant, Directory Access does not create directory domains. It

- configures connections with existing domains
- enables or disables service discovery protocols (AppleTalk, Rendezvous, SLP, and SMB)
- enables or disables directory protocols (LDAPv2, LDAPv3, NetInfo, and BSD configuration files)

In addition, Directory Access is available on both Mac OS X Servers and Mac OS X client computers, whereas Open Directory Assistant is available only on servers.

You'll find Directory Access in /Applications/Utilities/. For information about how to use it, see Chapter 2, "Directory Services."

Workgroup Manager

You use Workgroup Manager to administer user, group, and computer accounts; manage share points; and administer client management for Mac OS X users.

For information about using Workgroup Manager to administer user and group accounts, see Chapter 3, "Users and Groups." For information about using it to administer computer accounts and client management settings, see Chapter 6, "Client Management: Mac OS X," and Chapter 10, "Client Management: Mac OS 9 and OS 8." Chapter 4, "Sharing," describes how to use Workgroup Manager to manage share points.

Opening and Authenticating in Workgroup Manager

Workgroup Manager is installed in /Applications/Utilities/ when you install your server or set up an administrator computer. To open Workgroup Manager, click the Workgroup Manager icon in the Dock of Mac OS X Server or in the toolbar of Server Status:

- To open Workgroup Manager on the server you are using without authenticating, choose View Directories from the Server menu. You will have read-only access to information displayed in Workgroup Manager. To make changes, click the lock icon to authenticate as an administrator. This approach is most useful when you are administering different servers and working with different directory domains.
- To authenticate as an administrator for a particular server, enter the server's IP address or DNS name in the login window, or click Browse to choose from a list of servers. Specify the user name and password for an administrator of the server, then click Connect. Use this approach when you will be working most of the time with a particular server.

Major Workgroup Manager Tasks

After login, the user account window appears, with lists of user, group, and computer accounts in the server's local directory domain. Here is how to get started with the major tasks you'll be performing with this application:

- To administer user, group, or computer accounts, click the Accounts icon in the toolbar. See Chapter 3, “Users and Groups,” for information about user and group accounts and Chapter 6, “Client Management: Mac OS X,” for information about computer accounts.
- To work with preferences for managed users, groups, or computers, click the Preferences icon in the toolbar. See Chapter 6, “Client Management: Mac OS X,” for instructions.
- To work with share points, click the Sharing icon in the toolbar. See Chapter 4, “Sharing,” for instructions.
- To work with accounts in different directory domains at the same time, open multiple Workgroup Manager windows by choosing New Workgroup Manager Window from the Server menu.
- To open Server Status so you can monitor the status of a particular server, click the Status icon in the toolbar. See “Server Status” on page 61 for information about the Server Status application.
- To open Server Settings so you can work with a server's file, print, mail, Web, NetBoot, and network settings, choose Configure Services from the Server menu. See “Server Settings” on page 60 for information about the Server Settings application.
- To control the way Workgroup Manager lists users and groups, whether it should use SSL transactions, and other behaviors, choose Preferences from the Workgroup Manager menu.
- To customize the Workgroup Manager toolbar, choose Customize Toolbar from the View menu.
- To retrieve online information, use the Help menu. It provides help for server administrators about Workgroup Manager as well as other Mac OS X Server topics.

Server Settings

You use Server Settings to administer file, print, mail, Web, NetBoot, and network services on a server.

Server Settings is installed in /Applications/Utilities/ when you install your server or set up an administrator computer. To open Server Settings, click the Server Settings icon in the Dock of Mac OS X Server or choose Configure Services from the Server menu in Workgroup Manager.

To select a server to work with, enter its IP address or DNS name in the login window, or click Browse to choose from a list of servers. Specify the user name and password for an administrator, then click Connect.

Click the service modules arranged on the Server Settings tabs to choose commands that let you work with individual services:

- For administering file and print services, select the File & Print tab to access modules.
- For administering mail and Web service, select the Internet tab to access modules.
- For administering IP Firewall, DHCP, NetBoot, DNS, and SLP DA services, select the Network tab to access modules.
- To retrieve online information, use the Help menu. It provides help for server administrators about Server Settings as well as other Mac OS X Server topics.

Server Settings is not compatible with versions of Mac OS X Server earlier than version 10.2.

Server Status

You use Server Status to monitor the services running on Mac OS X Servers.

Server Status is installed in /Applications/Utilities/ when you install your server or set up an administrative computer. To open Server Status, click the Server Status icon in the Dock of Mac OS X Server or the Status icon in Workgroup Manager.

To select a server to monitor, click the Connect button in the Server Status toolbar. Enter the IP address or DNS name of the server you want to monitor in the login window, or click Browse to choose from a list of servers. Specify the user name and password for an administrator, then click Connect.

Select items in the Devices & Services list to monitor specific servers and services running on the servers:

- To review general status information for a particular server, select the server name.
- To review status information for a particular service running on a server, click the disclosure triangle next to the server name to see a list of its services. Then select the service of interest.
- To add a server to the Devices & Services list, click Connect in the toolbar and log in to the server. The next time you open Server Status, any server you have added is displayed in the Devices & Services list and can be monitored again by selecting a server in the list. If a server in the list appears grey, double-click the server or click the Reconnect button in the toolbar to log in again. Check the Add to Keychain option while you log in to enable autoreconnect the next time you open Server Status.
- To remove a server from the Devices & Services list, select the server, click the Disconnect button in the toolbar, and choose Remove From List from the Server menu.
- To control the way Server Status lists servers and services, how often status data is refreshed, and other behaviors, choose Preferences from the Server Status menu.
- To customize the Server Status toolbar, choose Customize Toolbar command from the View menu.

- To retrieve online information, use the Help menu. It provides help for server administrators about Server Status as well as other Mac OS X Server topics.

Macintosh Manager

You use Macintosh Manager to administer client management for Mac OS 8 and 9 client computers. You can use it locally (at the server) or remotely (from a Mac OS 9 or X computer on the same network as your Mac OS X Server).

Open Macintosh Manager by clicking its icon in the Dock. Log in using a server, Macintosh Manager, or workgroup administrator user name and password. As a server administrator, you automatically have global administrator privileges for Macintosh Manager.

See Chapter 10, “Client Management: Mac OS 9 and OS 8,” for more information.

NetBoot Administration Tools

There are several applications you use to administer NetBoot:

- NetBoot Desktop Admin lets you modify Mac OS 9 images.
- Network Image Utility lets you create and modify Mac OS X images.
- The DHCP/NetBoot module of Server Settings lets you save NetBoot images.

See Chapter 12, “NetBoot,” for information about these tools.

Network Install Administration Application

You use Package Maker to create Network Install packages.

See Chapter 13, “Network Install,” for information about this application.

Server Monitor

You use Server Monitor to monitor Xserve hardware and trigger email notifications when circumstances warrant attention. Server Monitor shows you information about the installed operating system, drives, power supply, enclosure and processor temperature, cooling blowers, security, and network.

Server Monitor is installed in /Applications/Utilities/ when you install your server or set up an administrator computer. Use the application to monitor local or remote servers:

- To specify the Xserve server to monitor, click Add Server, identify the server of interest, and enter user name and password information for an administrator of the server.
- Use the “Update every” pop-up menu to specify how often you want to refresh data.
- Use the Export Items and Import Items buttons to manage different lists of Xserve servers you want to monitor. The Merge Items button lets you consolidate lists into one.

- The system identifier lights on the front and back of an Xserve server light when service is required. Use Server Monitor to understand why the lights are on. You can also turn the lights on to identify a particular Xserve server in a rack of servers by selecting the server and clicking “system identifier light on” on the Info tab.
- You can set Server Monitor to notify you by email when an Xserve server’s status changes. For each server, you set up the conditions that you want notification about. The email message can come from Server Monitor or from the server.
- Server Monitor keeps logs of Server Monitor activity for each Xserve server. (The logs do not include system activity on the server.) The log shows, for example, the times Server Monitor attempted to contact the server, and whether a connection was successful. The log also shows server status changes. You can also use Server Monitor to get an Apple System Profiler report on a remote server.

Streaming Server Admin

To set up and manage QTSS, you use the Web-based Streaming Server Admin program.

Streaming Server Admin lets you easily create and serve playlists, customize general settings, monitor connected users, view log files, manage user and bandwidth usage, and relay a stream from one server to another for scalability.

To use Streaming Server Admin:

- 1 From Mac OS X Server, click the Streaming Server Admin icon in the Dock, then go to step 3. Alternatively, from a server with QTSS installed, open a Web browser. You can also use a Web browser from a remote Mac OS X computer.
- 2 Enter the URL for your Streaming Server Admin.
For example, `myserver.com:1220`
Replace “myserver.com” with the name of your Streaming Server computer. 1220 is the port number.
- 3 The first time you run Streaming Server Admin, the Setup Assistant prompts you for your user name and password.

To display online help information about using Streaming Server Admin, setting up secure administration (SSL), and setting up your server to stream hinted media, click the question mark button in the application. Information about QTSS is also available at the QuickTime Web site:

www.apple.com/quicktime/products/qtss/

Where to Find More Information

Regardless of your server administration experience, you may want to take advantage of the wide range of Apple customer training courses. To learn more, go to train.apple.com

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

The AppleCare support site's discussion boards are an additional source of information:

www.info.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 its 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/

Directory Services

Directory services provide a central repository for information about the systems, applications, and users in an organization. In education and enterprise environments, directory services are the ideal way to manage users and computing resources. Organizations with as few as 10 people can benefit by deploying directory services.

Directory services can be doubly beneficial. They centralize system and network administration, and they simplify a user's experience on the network. With directory services, information about all the users—such as their names, passwords, and preferences—as well as printers and other resources on a network can be maintained in a single location rather than on each computer on the network. Using directory services can reduce the system administrator's user management burden. In addition, users can log in to any authorized computer on the network. Anywhere a user logs in, the user's personal Desktop appears, customized for the user's individual preferences. The user always has access to personal files and can easily locate and use authorized network resources.

Apple has built an open, extensible directory services architecture, called Open Directory, into Mac OS X and Mac OS X Server. A Mac OS X Server or Mac OS X client computer can use Open Directory to retrieve authoritative information about users and network resources from a variety of sources:

- directory domains on the computer itself and on other Mac OS X Servers
- directory domains on other servers, including LDAP directory domains and Active Directory domains on non-Apple servers
- BSD configuration files located on the computer itself
- network services, such as file servers, that make themselves known with the Rendezvous, AppleTalk, SLP, or SMB service discovery protocols

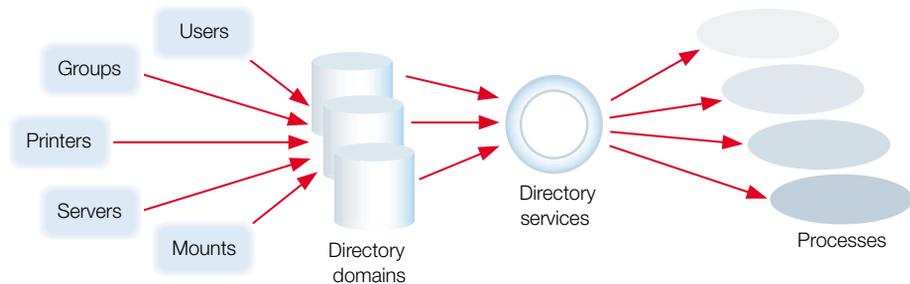
Mac OS 9 and Mac OS 8 managed clients also use Open Directory to retrieve some user information. For more information, see “How Macintosh Manager Works With Directory Services” on page 420 in Chapter 10, “Client Management: Mac OS 9 and OS 8.”

The Open Directory architecture also includes Open Directory Password Server. A Password Server can securely store and validate the passwords of users who want to log in to client computers on your network or use other network resources that require authentication. A Password Server can also enforce such policies as password expiration and minimum length.

To understand the information in this chapter, you should be comfortable with Mac OS X. You do not need advanced network administrator or UNIX experience to use directory services provided by Mac OS X Servers. If you want to integrate LDAP directories from other servers, you need to be familiar with LDAP. If you want to integrate Active Directory servers, you need to be familiar with Active Directory and LDAP. You need to be comfortable with UNIX if you want to integrate BSD configuration files.

Storage for Data Needed by Mac OS X

Directory services act as an intermediary between *directory domains*, which store information about users and resources, and the application and system software processes that want to use the information. A directory domain stores information in a specialized database that is optimized to handle a great many requests for information and to find and retrieve information quickly. Information may be stored in one directory domain or in several related directory domains.

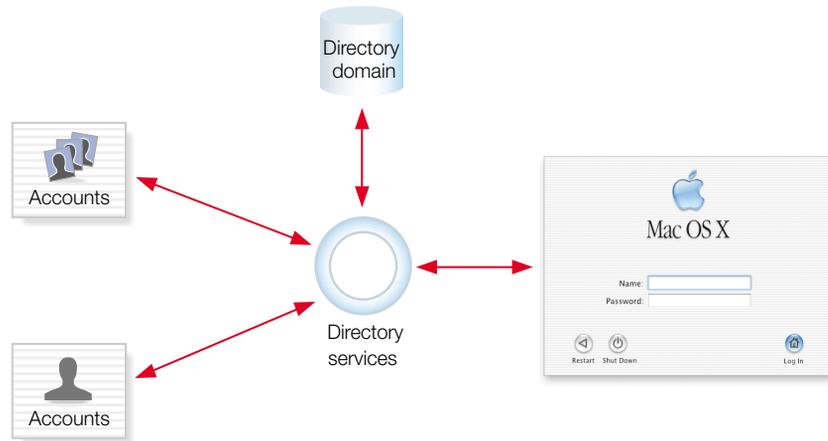


Processes running on Mac OS X computers can use directory services to save information in a directory domain. For example, when you set up a user account, the application that you use to do this has directory services store information about the user in a directory domain.

- *On a computer with Mac OS X version 10.2*, you use the My Account pane or the Accounts pane of System Preferences to set up user accounts that are valid only on the one computer.
- *On a computer with Mac OS X Server version 10.2*, you use the Accounts module of Workgroup Manager to set up user accounts that are valid on all Mac OS X computers on your network. You can specify additional user attributes in a network user account, such as the location of the user's home directory.

Whether you use Workgroup Manager or System Preferences to create a user account, the user information is stored in a directory domain.

When someone attempts to log in to a Mac OS X computer, the login process uses Mac OS X directory services—Open Directory—to validate the user name and password.

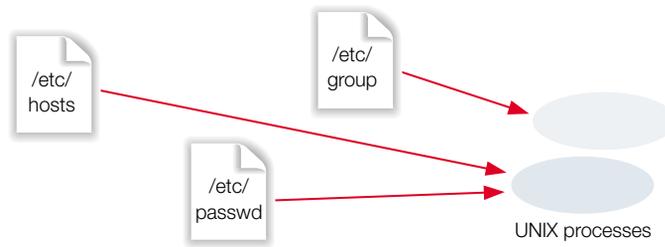


A Historical Perspective

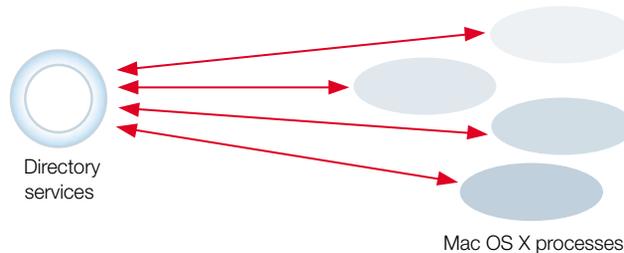
Like Mac OS X, Open Directory has a UNIX heritage. Open Directory provides access to administrative data that UNIX systems have generally kept in configuration files, which require much painstaking work to maintain. (Some UNIX systems still rely on configuration files.) Open Directory consolidates the data and distributes it for ease of access and maintenance.

Data Consolidation

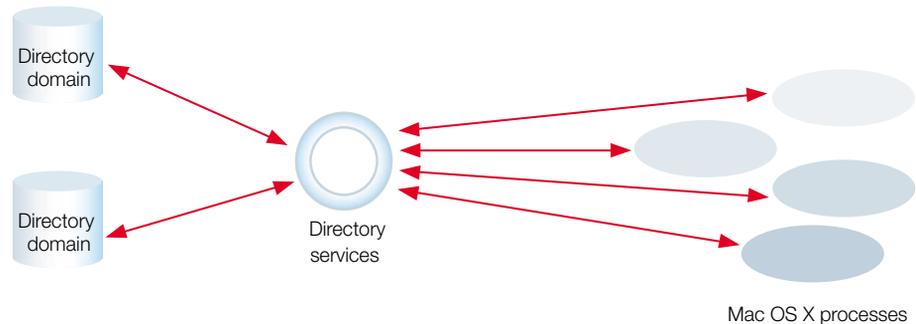
For years, UNIX systems have stored administrative information in a collection of files located in the `/etc` directory. This scheme requires each UNIX computer to have its own set of files, and processes that are running on a UNIX computer read its files when they need administrative information. If you're experienced with UNIX, you probably know about the files in the `/etc` directory—`group`, `hosts`, `hosts.eq`, `passwd`, and so forth. For example, a UNIX process that needs a user's password consults the `/etc/passwd` file, which contains a record for each user account. A UNIX process that needs group information consults the `/etc/group` file.



Open Directory consolidates administrative information, simplifying the interactions between processes and the administrative data they create and use.



Processes no longer need to know how and where administrative data is stored. Open Directory gets the data for them. If a process needs the location of a user's home directory, the process simply has Open Directory retrieve the information. Open Directory finds the requested information, and then returns it, insulating the process from the details of how the information is stored. If you set up Open Directory to access administrative data in several directory domains, Open Directory automatically consults them as needed.



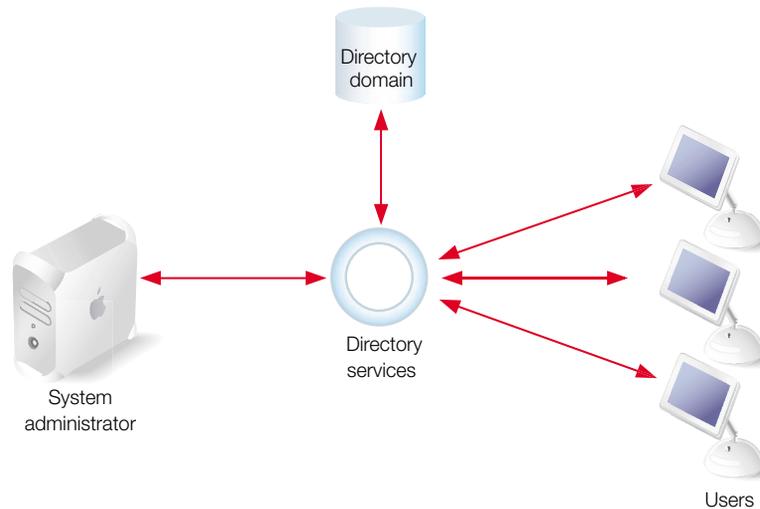
Some of the data stored in a directory domain is identical to data stored in UNIX configuration files. For example, the authentication attributes, home directory location, real name, user ID, and group ID—all stored in the user records of a directory domain—have corresponding entries in the standard `/etc/passwd` file. However, a directory domain stores much additional data to support functions that are unique to Mac OS X, such as support for managed clients and Apple Filing Protocol (AFP) directories.

Data Distribution

Another characteristic of UNIX configuration files is that the administrative data they contain is available only to the computer on which they are stored. Each computer has its own UNIX configuration files. With UNIX configuration files, each computer that someone wants to use must have that person's user account settings stored on it, and each computer must store the account settings for every person who may want to use the computer. To set up a computer's network settings, the administrator needs to go to the computer and directly enter the IP address and other information that identifies the computer on the network.

Similarly, when user or network information needs to be changed in UNIX configuration files, the administrator must make the changes on the computer where the files reside. Some changes, such as network settings, require the administrator to make the same changes on multiple computers. This approach becomes unwieldy as networks grow in size and complexity.

Open Directory solves this problem by letting you store administrative data in a directory domain that can be managed by a system administrator from one location. Open Directory lets you distribute the information so that it is visible on a network to the computers that need it and the administrator who manages it:



Uses of Directory Data

Open Directory makes it possible to consolidate and maintain network information easily in a directory domain, but this information has value only if application and system software processes running on network computers actually access the information. The real power of Open Directory is not that it provides directory services, but the fact that Mac OS X software accesses data through Open Directory.

Here are some of the ways in which Mac OS X system and application software use directory data:

- *Authentication.* As mentioned already, the Accounts module of Workgroup Manager or the Accounts pane of System Preferences creates user records in a directory domain, and these records are used to authenticate users who log in to Mac OS X computers. When a user specifies a name and a password in the Mac OS X login window, the login process asks Open Directory for the user record that corresponds to the name that the user specified. Open Directory finds the user record in a directory domain and retrieves the record.

- *Folder and file access.* After logging in successfully, a user can access files and folders. Mac OS X uses another data item from the user record—the user ID (UID)—to determine the user’s access privileges for a file or folder that the user wants to access. When a user accesses a folder or file, the file system compares this user’s UID to the UID assigned to the folder or file. If the UIDs are the same, the file system grants owner privileges (usually read and write privileges) to the user. If the UIDs are different, the user doesn’t get owner privileges.
- *Home directories.* Each user record in a directory domain stores the location of the user’s home directory, which is also known as the user’s home folder. This is where the user keeps personal files, folders, and preferences. A user’s home directory can be located on a particular computer that the user always uses or on a network file server.
- *Automount share points.* Share points can be configured to *automount* (appear automatically) in the /Network folder (the Network globe) in the Finder windows of client computers. Information about these automount share points is stored in a directory domain. *Share points* are folders, disks, or disk partitions that you have made accessible over the network.
- *Mail account settings.* Each user’s record in a directory domain specifies whether the user has mail service, which mail protocols to use, how to present incoming mail, whether to alert the user when mail arrives, and more.
- *Resource usage.* Disk, print, and mail quotas can be stored in each user record of a directory domain.
- *Managed client information.* A user’s personal preference settings, as well as preset preferences that affect the user, are stored in a directory domain.
- *Group management.* In addition to user records, a directory domain also stores group records. Each group record affects all users who are in the group. Information in group records specifies preferences settings for group members. Group records also determine access to files, folders, and computers.

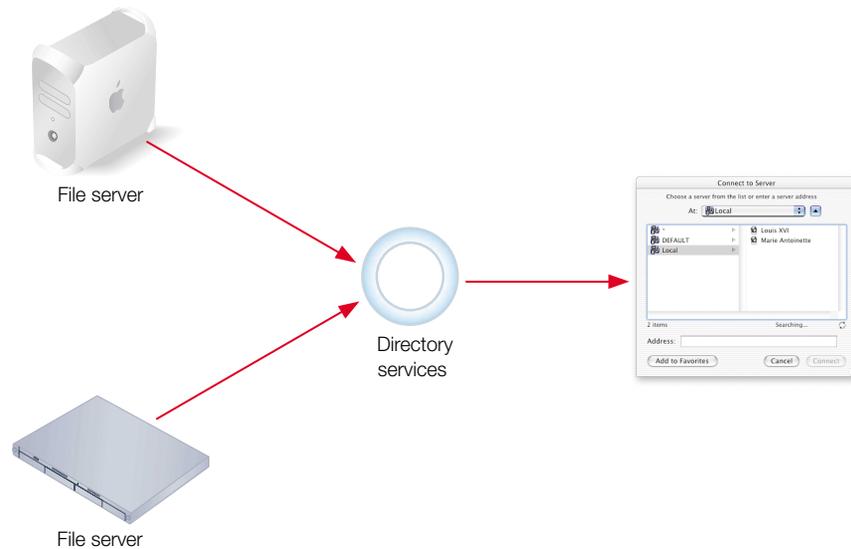
Inside a Directory Domain

Information in a directory domain is organized into record types, which are specific categories of records, such as users, machines, and mounts. For each record type, a directory domain may contain any number of records. Each record is a collection of attributes, and each attribute has one or more values. If you think of each record type as a spreadsheet that contains a category of information, then records are like the rows of the spreadsheet, attributes are like spreadsheet columns, and each spreadsheet cell contains one or more values.

For example, when you define a user by using the Accounts module of Workgroup Manager, you are creating a user record (a record of the user's record type). The settings that you configure for the user—short name, full name, home directory location, and so on—become values of attributes in the user record. The user record and the values of its attributes reside in a directory domain.

Discovery of Network Services

Open Directory can provide more than administrative data from directories. Open Directory can also provide information about services that are available on the network. For example, Open Directory can provide information about file servers that are currently available.



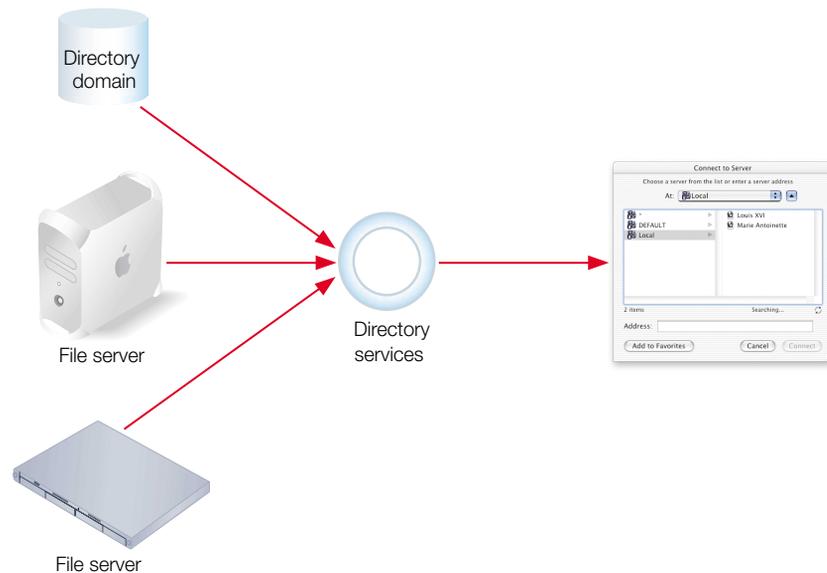
Information about file servers and other services tends to change much more frequently than information about users. Therefore, information about network services typically isn't stored in directory domains. Instead, information about file servers and other network servers is discovered as the need arises.

Open Directory can discover network services that make their existence and whereabouts known. Services make themselves known by means of standard protocols. Open Directory supports the following service discovery protocols:

- Rendezvous, the Apple protocol that uses multicast DNS
- AppleTalk, the legacy Mac OS protocol for file services
- Service Location Protocol (SLP), an open standard for discovering file and print services
- Server Message Block (SMB), the protocol used by Microsoft Windows

In fact, Open Directory can provide information about network services both from service discovery protocols and from directory domains. To accomplish this, Open Directory simply asks all its sources of information for the type of information requested by a Mac OS X process. The sources that have the requested type of information provide it to Open Directory, which collects all the provided information and hands it over to the Mac OS X process that requested it.

For example, if Open Directory requests information about file servers, the file servers on the network respond via service discovery protocols with their information. A directory domain that contains relatively static information about some file servers also responds to the request. Open Directory collects the information from the service discovery protocols and the directory domains.



When Open Directory requests information about a user, service discovery protocols don't respond because they don't have user information. (Theoretically, AppleTalk, Rendezvous, SMB, and SLP could provide user information, but in practice they don't have any user information to provide.) The user information that Open Directory collects comes from whatever sources have it—from directory domains.

Directory Domain Protocols

Administrative data needed by directory services is stored on Mac OS X Servers in Open Directory databases. An Open Directory database is one type of directory domain. Open Directory can use either of two protocols to store and retrieve directory data:

- Lightweight Directory Access Protocol (LDAP), an open standard commonly used in mixed environments
- NetInfo, the Apple directory services protocol for Mac OS X

The directory services of Mac OS X version 10.2—Open Directory—can also store and retrieve administrative data that resides in existing directory domains on other servers. Open Directory can read and write data in the following domains:

- Shared NetInfo domains on other Mac OS X computers (servers or clients)
- OpenLDAP directories on various UNIX servers
- Active Directory domains on Windows servers
- Other LDAPv3-compliant directories that are configured to allow remote administration and read and write access

In addition, Open Directory can retrieve but not store administrative data in the following domains:

- BSD configuration files located on the Mac OS X Server
- LDAPv2 domains and read-only LDAPv3 domains on other servers

Local and Shared Directory Domains

Where you store your server's user information and other administrative data is determined by whether the data needs to be shared.

Local Data

Every Mac OS X computer has a local directory domain. A local domain's administrative data is visible *only* to applications and system software running on the computer where the domain resides. It is the first domain consulted when a user logs in or performs some other operation that requires data stored in a directory domain.

When the user logs in to a Mac OS X computer, Open Directory searches the computer's local directory domain for the user's record. If the local directory domain contains the user's record (and the user typed the correct password), the login process proceeds and the user gets access to the computer.



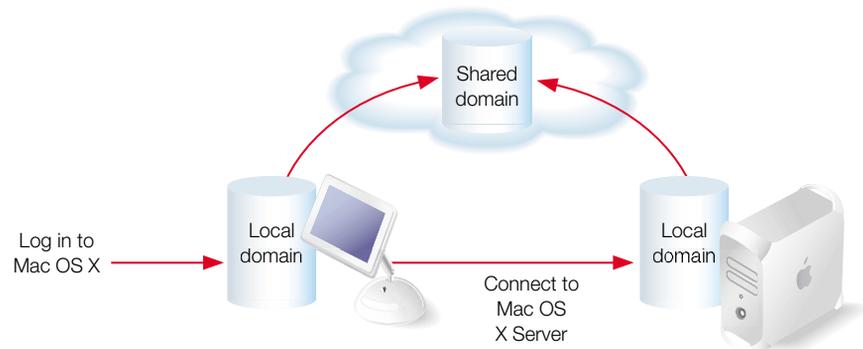
After login, the user may choose Connect To Server from the Go menu and connect to a file server on a computer running Mac OS X Server. In this case, Open Directory on the server searches for the user's record in the server's local directory domain. If the server's local directory domain has a record for the user (and the user types the correct password), the server grants the user access to the file services.

When you first set up a Mac OS X computer, its local directory domain is automatically created and populated with records. For example, a user record is created for the user who performed the installation. It contains the user name and password entered during setup, as well as other information, such as a unique ID for the user and the location of the user's home directory.

Shared Data

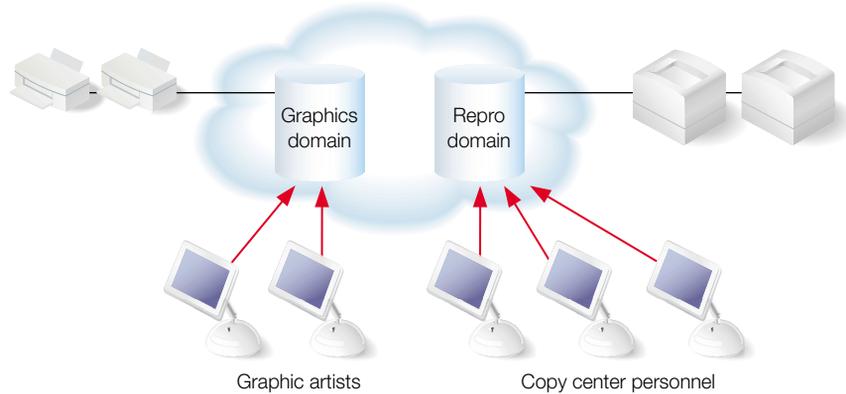
While Open Directory on any Mac OS X computer can store administrative data in the computer's local directory domain, the real power of Open Directory is that it lets multiple Mac OS X computers share administrative data by storing the data in shared directory domains. When a computer is configured to use a shared domain, any administrative data in the shared domain is also visible to applications and system software running on that computer.

If Open Directory does not find a user's record in the local domain of a Mac OS X computer, Open Directory automatically searches for the user's record in any shared domains to which the computer has access. In the following example, the user can access both computers because the shared domain accessible from both computers contains a record for the user.



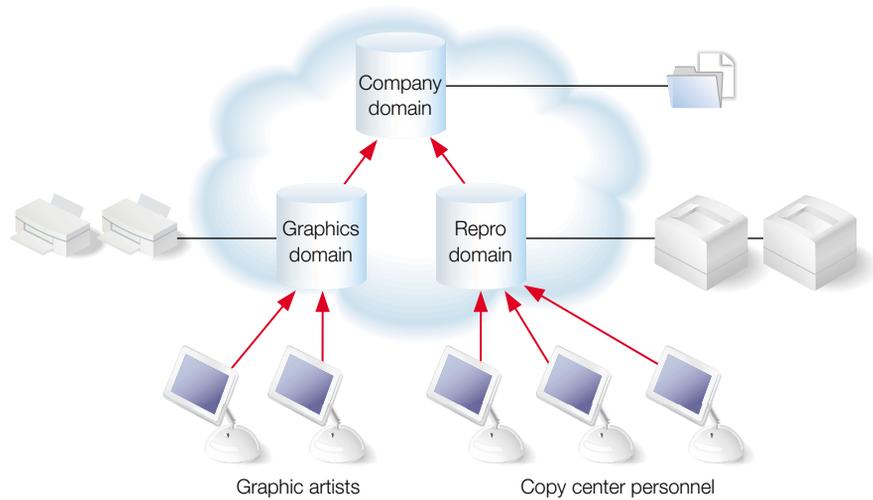
Shared domains generally reside on Mac OS X Servers, because servers are equipped with the tools, such as Workgroup Manager and Server Settings, that facilitate managing network resources and network users.

Similarly, you can make network resources such as printers visible to certain computers by setting up printer records in a shared domain accessed by those computers. For example, graphic artists in a company might need to access color printers, while copy center personnel need to use high-speed laser printers. Rather than configuring printer access for each computer individually, you could use the Print module of Server Settings to add printers to two shared domains: Graphics and Repro.



Printers visible in the Print Center of graphic artists' computers would be those in the Graphics domain, while printers in the Repro domain would be visible to computers used by copy center personnel. Printers that have records in shared domains appear in the Directory Services printer list in Print Center.

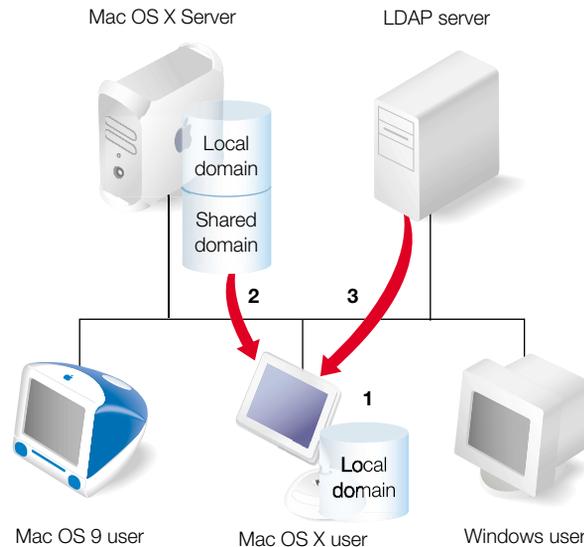
While some devices may need to be used only by specific departments, other resources, such as personnel forms, may need to be shared by all employees. You could make a folder of those forms available to everybody by setting up a share point for the folder in another shared domain that all computers can access.



The shared domain at the top of a hierarchy of directory domains is sometimes called the *root* domain.

Shared Data in Existing Directory Domains

Some organizations—such as universities and worldwide corporations—maintain user information and other administrative data in directory domains on UNIX or Windows servers. Open Directory can be configured to search these non-Apple domains as well as shared Open Directory domains of Mac OS X Servers.



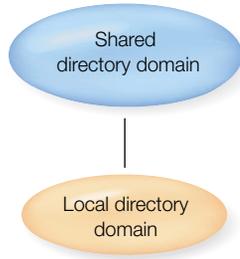
When a user logs in to a computer on your network, Open Directory still searches for the user in the computer's local domain and in shared domains on Mac OS X Servers. But if the user is not found and Open Directory has been configured to search an LDAP domain on a UNIX server, Open Directory consults the LDAP domain for information about the user.

Directory Domain Hierarchies

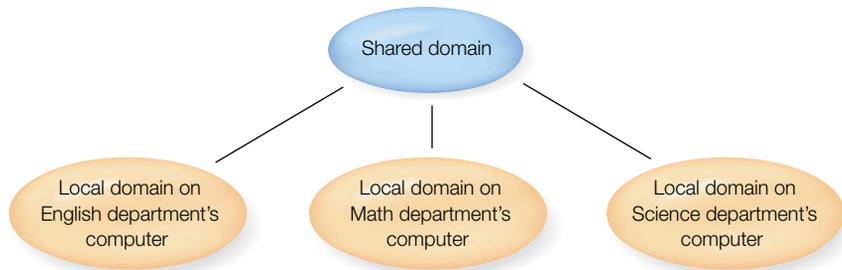
Local and shared domains are organized into hierarchies, tree-like topologies that have a shared domain at the top and local domains at the bottom of the tree. A hierarchy can be as simple as a local domain and a shared domain, or it can contain more shared domains.

Two-Level Hierarchies

The simplest hierarchy is a two-level hierarchy:

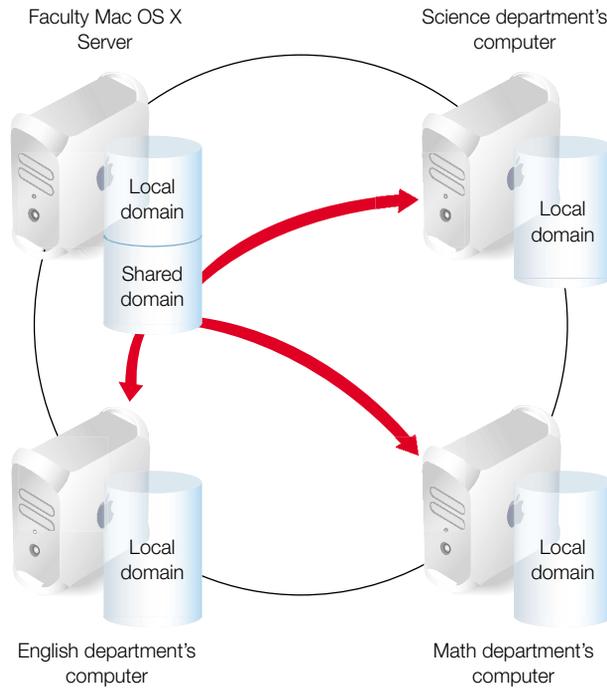


Here's a scenario in which a two-level hierarchy might be used:



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 shared domain, in which all the instructors are defined. Instructors, as members of the shared 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.

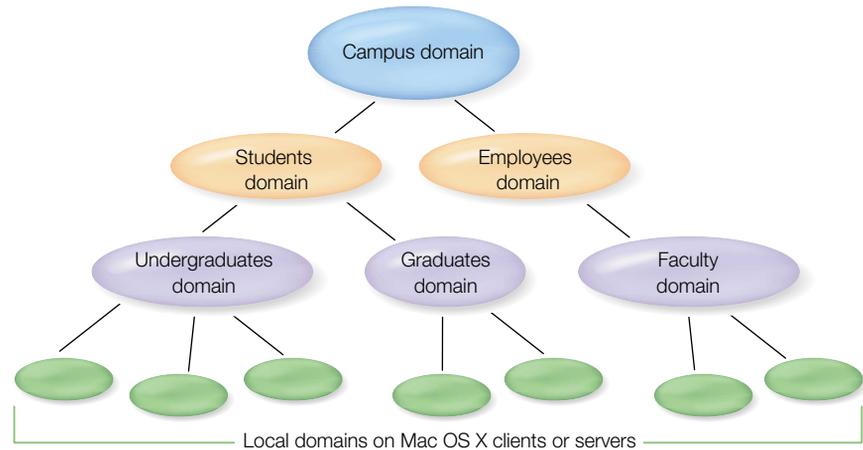
While local domains reside on their respective servers, a shared domain can reside on any Mac OS X Server accessible from the local domain's computer. In this example, the shared domain can reside on any server accessible from the departmental servers. It can reside on one of the departmental servers, 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 shared domain. In this example, there is only one shared domain, but in more complex hierarchies, there may be many shared domains.

More Complex Hierarchies

Open Directory 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 Campus domain can use Mac OS X computers on which any of the local domains reside. A student defined in the Students domain can log in to any Mac OS X computers that are below the Graduates domain or Undergraduates domain.

A directory domain hierarchy affects which Mac OS X computers can see particular administrative data. The “subtrees” of the hierarchy essentially hide information from other subtrees in the hierarchy. In the education example, computers using the subtree that includes the Graduates domain do not have access to records in the Undergraduates domain. But records in the Campus domain are visible to any computer.

Directory domain visibility depends on the computer, not the user. So when a user logs in to a different computer, administrative data from different directory domains may be visible to that computer. In the education scenario described here, an undergraduate can log in to a graduate student's computer if the undergraduate's user record resides in the Students domain. But the devices that are defined in the Undergraduates domain are not visible unless they are also defined in the Graduates, Students, or Campus domain.

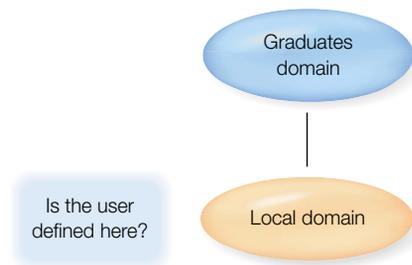
You can affect an entire network or just a group of computers by choosing which domain to publish administrative data in. The higher the administrative data resides in a directory domain hierarchy, the fewer places it needs to be changed as users and system resources change. Probably the most important aspect of directory services for administrators is planning directory domains and hierarchies. These should reflect the resources you want to share, the users you want to share them among, and even the way you want to manage your directory data.

Search Policies for Directory Domain Hierarchies

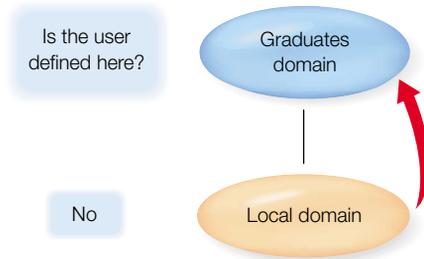
In a hierarchy of directory domains, each Mac OS X computer has a *search policy* that specifies the order in which Open Directory searches the domains. A search policy, also known as a search path, is simply a list of directory domains. On a Mac OS X computer, Open Directory goes down this list of directory domains whenever an application or system software running on the computer needs administrative data. The list of directory domains defines the computer's search policy. The search policy effectively establishes the computer's place in the hierarchy.

A computer's local directory domain is always first on the list. It may be followed by shared Open Directory domains on Mac OS X Servers and LDAP domains on other servers. It may also include a set of BSD configuration files that are on the computer.

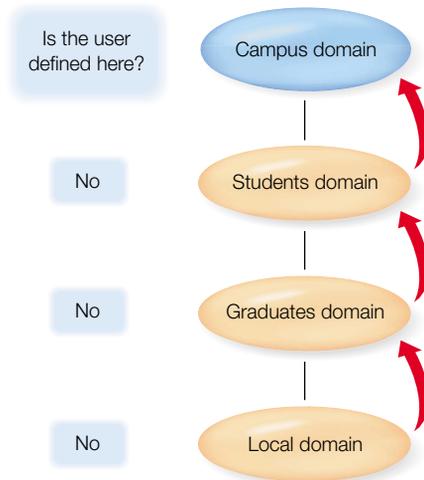
For example, when someone tries to log in to a Mac OS X computer, Open Directory searches the computer's local domain for the user's record. The local directory domain is always first on a computer's search policy.



If the local domain does not contain the user's record, Open Directory goes to the next directory domain in the search policy.



If the second directory domain also does not contain the user's record, Open Directory searches the remaining directory domains in the search policy one by one until it searches the last shared domain.



The Automatic Search Policy

Initially, every computer with Mac OS X version 10.2 is set to use an *automatic search policy*. It consists of three parts, two of which are optional:

- local directory domain
- shared NetInfo domains (optional)
- shared LDAPv3 domains (optional)

A computer's automatic search policy always begins with the computer's local directory domain.

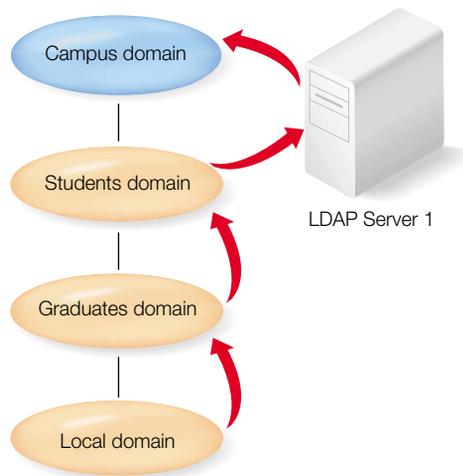
Next the automatic search policy looks at the binding of shared NetInfo domains. The computer's local domain may be bound to a shared NetInfo domain, which may in turn be bound to another shared NetInfo domain, and so on. The NetInfo binding, if any, constitutes the second part of the automatic search policy. See "Configuring NetInfo Binding" on page 111 for additional information.

The third and final part of a computer's automatic search policy consists of shared LDAPv3 domains. They are included only if the computer uses a DHCP service that's configured to supply the addresses of one or more LDAPv3 servers. The DHCP service of Mac OS X Server can supply LDAPv3 servers. See "Setting the LDAP Server for DHCP Clients" on page 479 in Chapter 11, "DHCP Service."

A computer's automatic search policy may change if the computer is moved to a part of the network served by a different DHCP service. When the user logs in at the new location, the computer connects to the new DHCP service. The new DHCP service may change the NetInfo binding and may supply a different list of LDAPv3 servers than the DHCP service at the former location.

Custom Search Policies

If you don't want a Mac OS X version 10.2 computer—server or client—to use the automatic search policy supplied by DHCP, you can define a custom search policy for the computer.



In this scenario, a custom search policy specifies that LDAP Server 1 be consulted when a user record or other administrative data cannot be found in the directory domains of the automatic search policy. The custom search policy also specifies that if the user information or other administrative data is not found on the LDAP server, a shared Open Directory domain named "Campus" is searched.

Directory Domain Planning

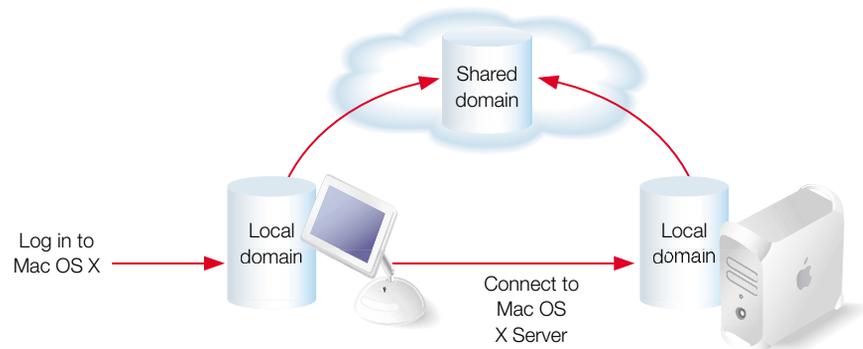
Keeping information in shared directory domains gives you more control over your network, allows more users access to the information, and makes maintaining the information easier for you. But the amount of control and convenience depends on the effort you put into planning your shared domains. The goal of directory domain planning is to design the simplest hierarchy of shared domains that gives your Mac OS X users easy access to the network resources they need *and* minimizes the time you spend maintaining administrative data.

General Planning Guidelines

If you do not need to share user and resource information among multiple Mac OS X computers, there is very little directory domain planning necessary. Everything can be accessed from local directory domains. Just ensure that all individuals who need to use a particular Mac OS X computer are defined as users in the local directory domain on the computer.

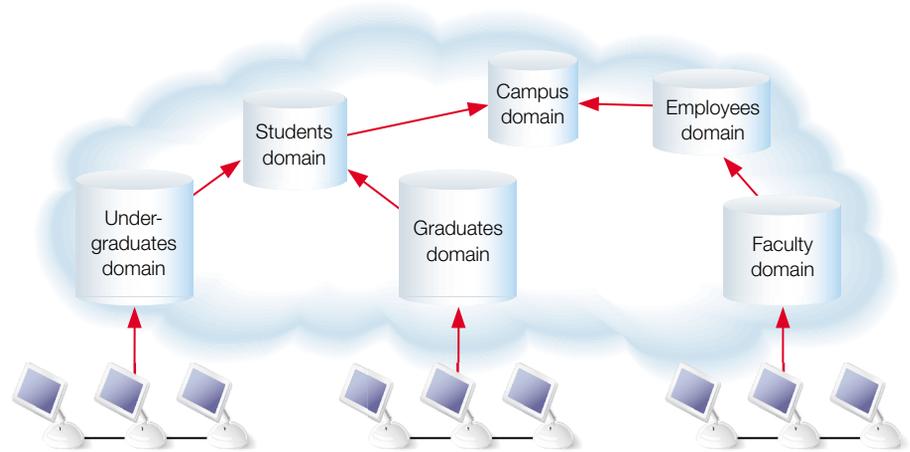


If you want to share information among Mac OS X computers, you need to set up at least one shared domain.



A hierarchy this simple may be completely adequate when all your network computer users share the same resources, such as printers and share points for home directories, applications, and so forth.

Larger, more complex organizations can benefit from a deeper directory domain hierarchy.



Controlling Data Accessibility

Hierarchies that contain several shared domains let you make directory information visible to only subsets of a network's computers. In the foregoing example hierarchy, the administrator can tailor the users and resources visible to the community of Mac OS X computers by distributing directory information among six shared domains.

If you want all computers to have access to certain administrative data, you store that data in the shared domain at the top of your hierarchy, where all computers can access it. To make some data accessible only to a subset of computers, you store it in a shared domain that only those computers can access.

You might want to set up multiple shared directory domains to support computers used by specific groups within an organization. For example, you might want to make share points containing programming applications and files visible only to engineering computers. On the other hand, you might give technical writers access to share points that store publishing software and document files. If you want all employees to have access to each other's home directories, you would store mount records for all the home directories in the topmost shared domain.

Simplifying Changes to Data in Directory Domains

If you need more than one shared directory domain, you should organize your hierarchy of shared domains to minimize the number of places data has to change over time. You should also devise a plan that addresses how you want to manage such ongoing events as

- new users joining and leaving your organization
- file servers being added, enhanced, or replaced

- printers being moved among locations

You'll want to try to make each directory domain applicable to all the computers that use it so you don't have to change or add information in multiple domains. In the education hierarchy example, all students may have user records in the Students domain and all employees have accounts in the Employees domain. As undergraduate students leave or become graduate students, or as employees are hired or retire, the administrator can make adjustments to user information simply by editing one domain.

If you have a widespread or complex hierarchy of directory domains in a network that is managed by several administrators, you need to devise strategies to minimize conflicts. For example, you can predefine ranges of user IDs (UIDs) to avoid inadvertent file access. (For more information, see "Defining User IDs" on page 144 in Chapter 3, "Users and Groups.")

Identifying Computers for Hosting Shared Domains

If you need more than one shared domain, you need to identify the computers on which shared domains should reside. Shared domains affect many users, so they should reside on Mac OS X Servers that have the following characteristics:

- restricted physical access
- limited network access
- equipped with high-availability technologies, such as uninterruptible power supplies

You should select computers that will not be replaced frequently and that have adequate capacity for growing directory domains. While you can move a shared domain after it has been set up, you may need to reconfigure the search policies of computers that bind to the shared domain so that their login hierarchies remain intact.

Open Directory Password Server

Besides providing directory services on Mac OS X Servers and other Mac OS X computers, Open Directory can also provide authentication services. An Open Directory Password Server can store and validate user passwords for login and other network services that require authentication. A Password Server supports basic authentication as well as authentication protocols that protect the privacy of a password during transmission on the network. A Password Server lets you set up specific password policies for each user, such as automatic password expiration and minimum password length.

Your Mac OS X Server can host a Password Server, or it can get authentication services from a Password Server hosted by another Mac OS X Server.

Authentication With a Password Server

When a user's account is configured to use a Password Server, the user's password is not stored in a directory domain. Instead, the directory domain stores a unique password ID assigned to the user by the Password Server. To authenticate a user, directory services pass the user's password ID to the Password Server. The Password Server uses the password ID to find the user's actual password and any associated password policy.

For example, the Password Server may locate a user's password but discover that it has expired. If the user is logging in, the login window asks the user to replace the expired password. Then the Password Server can authenticate the user.

A Password Server can't authenticate a user during login on a computer with Mac OS X version 10.1 or earlier.

You'll find more information about configuring user accounts to use a Password Server in "Understanding Password Validation" on page 189 of Chapter 3, "Users and Groups."

Network Authentication Protocols

The Password Server is based on a standard known as Simple Authentication and Security Layer (SASL). This standard enables a Password Server to support the wide range of network user authentication protocols used by various network services of Mac OS X Server, such as mail service and file services. Here are a few of the network authentication protocols that the Password Server supports:

- CRAM-MD5
- MD5
- APOP
- NT and LAN Manager (for SMB)
- SHA-1
- DHX
- AFP 2-Way Random
- WebDAV Digest

Password Server Database

The Password Server maintains a record for each user that includes the following:

- Password ID, a 128-bit value assigned when the password is created. The value includes a key for finding a user's Password Services record.

- The password, stored in recoverable or hashed form. The form depends on the network authentication protocols enabled for the Password Server (using Open Directory Assistant). If APOP or 2-Way Random is enabled, the Password Server stores a recoverable (encrypted) password. If neither of these methods is enabled, only hashes of the passwords are stored.
- Data about the user that is useful in log records, such as the user's short name.
- Password policy data.

Password Server Security

The Password Server stores passwords, but never allows passwords to be read. Passwords can only be set and verified. Malicious users who want to gain access to your server must try to log in over the network. Invalid password instances, logged by the Password Server, can alert you to such attempts.

Using a Password Server offers flexible and secure password validation, but you need to make sure that the server on which a Password Server runs is secure:

- Set up Password Servers on a server that is not used for any other activity.
- Since the load on a Password Server is not particularly high, you can have several (or even all) of your Open Directory server domains share a single Password Server.
- Set up IP firewall service so nothing is accepted from unknown ports. Password Server uses a well-known port.
- Make sure that the Password Server's computer is located in a physically secure location, and don't connect a keyboard or monitor to it.
- Equip the server with an uninterruptible power supply.

The Password Server must remain available to provide authentication services. If the Password Server goes down, password validation cannot occur, because you cannot replicate a Password Server.

Overview of Directory Services Tools

The following applications help you set up and manage directory domains and Password Servers.

- *Open Directory Assistant*. Use to create and configure shared or standalone Open Directory domains (NetInfo or LDAPv3) and to set up Open Directory Password Servers. Located in /Applications/Utilities.
- *Directory Access*. Use to enable or disable individual directory service protocols; define a search policy; configure connections to existing LDAPv3, LDAPv2, and NetInfo domains; and configure data mapping for LDAPv3 and LDAPv2 domains. Located in /Applications/Utilities.

- *Server Status*. Use to monitor directory services and view directory services logs. Located in /Applications/Utilities.

Experts can also use the following applications to manage directory domains:

- *Property List Editor*. Use to add BSD configuration files that you want Open Directory to access for administrative data, and change the mapping of the data in each BSD configuration file to specific Mac OS X record types and attributes. Located in /Developer/Applications if you have installed the developer tools from the Developer Tools CD.
- *NetInfo Manager*. Use to view and change records, attributes, and values in an Open Directory domain (LDAPv3 or NetInfo) or in a NetInfo domain; manage a NetInfo hierarchy; and back up and restore a NetInfo domain. Located in /Applications/Utilities.
- *Terminal*. Open to use UNIX command-line tools that manage NetInfo domains. Located in /Applications/Utilities.

Setup Overview

Here is a summary of the major tasks you perform to set up and maintain directory services. See the pages indicated for detailed information about each task.

Step 1: Before you begin, do some planning

See “Before You Begin” on page 91 for a list of items to think about before you start configuring directory domains.

Step 2: Set up Open Directory domains and Password Servers

Create shared directory domains on the Mac OS X Servers that you want to host them. At the same time, set up Open Directory Password Servers. See the following sections:

- “Setting Up an Open Directory Domain and Password Server” on page 92
- “Deleting a Shared Open Directory Domain” on page 93

Step 3: Set up access to directory domains on other servers

If some of your user information and other administrative data will not reside in Open Directory domains, you must make sure your other sources of data are set up for Mac OS X. For instructions, see the following sections of this chapter:

- “Configuring Access to Existing LDAPv3 Servers” on page 98
- “Using an Active Directory Server” on page 104
- “Accessing an Existing LDAPv2 Directory” on page 106
- “Using NetInfo Domains” on page 110
- “Using Berkeley Software Distribution (BSD) Configuration Files” on page 115

Step 4: Implement search policies

Set up search policies so that all computers have access to the shared directory domains they need. Note that if all computers have Mac OS X version 10.2 and can use the automatic search policy, there is nothing to set up. Otherwise, see “Setting Up Search Policies” on page 94.

If your network includes computers with Mac OS X versions earlier than 10.2, configure the local domain on each of them so that it binds to a shared NetInfo domain. See “Using NetInfo Domains” on page 110.

Step 5: Configure Open Directory service protocols (optional)

You may want to disable some of the protocols that Open Directory uses to access directory domains and to discover network services. See “Configuring Open Directory Service Protocols” on page 93.

Before You Begin

Before setting up directory services for the first time:

- Understand why clients need directory data, as discussed in the first several sections of this chapter.
- Assess your server access requirements.

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

Users whose information can be managed most easily on a server should be defined in a shared Open Directory domain on a Mac OS X Server. Some of these users may instead be defined in Active Directory domains or LDAP domains on other servers.

For more information, see “Local and Shared Directory Domains” on page 74 and “Directory Domain Hierarchies” on page 78.

- Understand search policies, as described in “Search Policies for Directory Domain Hierarchies” on page 82.
- Design the hierarchy of shared directory domains.

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

“Directory Domain Planning” on page 85 provides some guidelines that will help you decide what your directory domain hierarchy should look like.
- Assess your authentication needs.

Decide whether to use an Open Directory Password Server. Decide which Mac OS X Server will host the Password Server. See “Open Directory Password Server” on page 87.

- Consider the best equipment and location for your servers.
Choose computers and locations that are reliable and accessible.
If possible, use a dedicated Mac OS X Server for directory services.
Make the server physically secure. It shouldn't have a keyboard or monitor, especially if it hosts a Password Server.
- Pick server administrators very carefully. Give only trusted people administrator passwords.
Have as few administrators as possible. Don't delegate administrator access for minor tasks, such as changing settings in a user record.
Always remember: directory information is authoritative. It vitally affects everyone whose computers use it.

Setting Up an Open Directory Domain and Password Server

You can use the Open Directory Assistant application to configure how a Mac OS X Server works with directory information and a Password Server. This application can configure a server to use a directory domain in one of the following ways:

- Use a shared directory domain hosted by another server.
- Host a shared Open Directory domain.
- Use only the server's own local directory domain.
- Delete the server's shared directory domain.

In addition, Open Directory Assistant can configure a server to use a Password Server in one of the following ways:

- Use an existing Password Server.
- Host a Password Server.
- Don't use a Password Server.

Open Directory Assistant runs automatically as part of the installation and setup process of Mac OS X Server. At any other time, you can open Open Directory Assistant from the Finder.

To configure how your server works with directory information and a Password Server:

- 1 Open the Open Directory Assistant application.
It is located in the /Applications/Utilities folder.
- 2 Enter the connection and authentication information for the Mac OS X Server that you want to configure, then click Connect.

For Address, enter the DNS name or IP address of the server that you want to configure.

For User Name, enter the user name of an administrator on the server.

For Password, enter the password for the user name you entered.

- 3 Follow the self-guided steps for configuring the server's use of a directory domain and a Password Server.

Deleting a Shared Open Directory Domain

You can delete a shared Open Directory domain that is hosted by a Mac OS X Server. Use Open Directory Assistant to do this.

Warning When you delete a directory domain, all user account information and other administrative data that it contains is lost.

To delete a shared directory domain hosted by a Mac OS X Server:

- 1 Start Open Directory Assistant.
- 2 Enter the connection and authentication information for the Mac OS X Server that hosts the shared domain you want to delete, then click Connect.

For Address, enter the DNS name or IP address of the server.

For User Name, enter the user name of an administrator on the server.

For Password, enter the password for the user name you entered.

- 3 Choose Delete Hosted Domain from the Domain menu.

After deleting a shared domain that is supplied automatically by DHCP, you must remove it from the DHCP service. Otherwise client computers may pause for long periods of time while trying to access the deleted domain. For instructions, see “Setting the LDAP Server for DHCP Clients” on page 479 in Chapter 11, “DHCP Service.”

Configuring Open Directory Service Protocols

Open Directory uses many protocols to access administrative data in directory domains and discover services on the network. You can enable or disable each of the protocols individually by using the Directory Access application. The protocols include

- AppleTalk, the legacy Mac OS protocol for file and print services
- BSD Configuration Files, the original method still used by some organizations for accessing administrative data on UNIX computers
- Lightweight Directory Access Protocol version 2 (LDAPv2), an open standard that Open Directory can use to access (read-only) directory domains on a variety of servers

- LDAPv3, a newer version of the popular directory services protocol, which Open Directory uses to access (read and write) data in Open Directory domains on computers and servers with Mac OS X version 10.2, Active Directory domains on Windows servers, and directory domains on various other servers
- NetInfo, an Apple directory services protocol that Open Directory can use to access (read and write) data in directory domains on all Mac OS X computers
- Rendezvous, an Apple protocol for discovering file, print, and other services on Internet Protocol (IP) networks
- Service Location Protocol (SLP), an open standard for discovering file and print services on IP networks
- Server Message Block (SMB), a protocol used by Microsoft Windows for file and print services

If you disable a protocol on a computer, Open Directory does not use it for directory access or service discovery on the computer. Other network services may still use the protocol, however. For example, if you disable the AppleTalk protocol, Open Directory does not use it to discover file servers, but you can still connect to an AppleTalk file server if you know its URL.

To enable or disable protocols used by Open Directory:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Click the checkbox next to the protocol that you want to enable or disable.
- 4 Click Apply.

Setting Up Search Policies

This section describes how to configure the search policy that Open Directory uses when it retrieves authentication information and other administrative data from directory domains. The search policy can also include protocols for discovering services on the network, such as file and print services.

A Mac OS X computer—server or client—actually has more than one search policy. The authentication search policy is used to find authentication information and most other administrative data. The contacts search policy is used by mail, address book, personal information manager, and similar applications to locate name, address, and other contact information.

You can configure the authentication search policy for a Mac OS X Server or other Mac OS X computer by using the Directory Access application. You can use the same application to configure the computer's contacts search policy. (The Open Directory Assistant application also configures the authentication search policy of a Mac OS X Server, but does not offer as many options as Directory Access.)

You can configure the search policy of the computer on which you are running Directory Assistant as follows:

- Use the automatic search policy—shared NetInfo domains, list of LDAP servers supplied by DHCP, or both.
- Define a custom search policy for the computer if it needs to search additional directory servers, BSD configuration files, or service discovery protocols.
- Use only the computer's local directory domain.

Using the Automatic Search Policy

You can configure a Mac OS X computer to use the automatic search policy. This is the default configuration. You can configure a computer to use the automatic search policy by using the Directory Access application on the computer.

The automatic search policy always includes the local directory domain. The automatic search policy also includes shared NetInfo domains to which the computer is bound and shared LDAPv3 domains supplied by DHCP. The shared NetInfo domains are optional, as are the shared LDAPv3 domains. For more information, see “Using NetInfo Domains” on page 110 and “Setting the LDAP Server for DHCP Clients” on page 479.

To use the automatic search policy supplied by DHCP:

- 1 In Directory Access, click the Authentication tab or the Contacts tab.
Click Authentication to configure the search policy used for authentication and most other administrative data.
Click Contacts to configure the search policy used for contact information in some mail, address book, and personal information manager applications.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Choose Automatic from the Search pop-up menu, then click Apply.

Defining a Custom Search Policy

You can configure a Mac OS X computer to search specific Open Directory servers, LDAP servers, NetInfo domains, BSD configuration files, or directory service protocols in addition to the servers in the automatic search policy. You define a custom search policy with the Directory Access application on the computer that you want to configure.

Note: Make sure the computer has been configured to access the LDAP servers, Active Directory servers, NetInfo domains, and BSD configuration files that you want to add to the search policy. For instructions, see the subsequent sections of this chapter.

To define a custom search policy for the computer:

- 1 In Directory Access, click the Authentication tab or the Contacts tab.
Click Authentication to configure the search policy used for authentication and most other administrative data.
Click Contacts to configure the search policy used for contact information in some mail, address book, and personal information manager applications.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Choose “Custom path” from the Search pop-up menu.
- 4 Click Add.
- 5 Select from the list of available directories and click Add.
To add multiple directories, select more than one and click Add.
- 6 Change the order of the listed directory domains as needed, and remove listed directory domains that you don’t want in the search policy.
Move a listed directory domain by dragging it up or down.
Remove a listed directory domain by selecting it and clicking Remove.
- 7 Click Apply.

Using a Local Directory Search Policy

If you want to limit the access that a computer has to authentication information and other administrative data, you can restrict the computer’s authentication search policy to the local directory domain. If you do this, users without local accounts on the computer will be unable to log in or authenticate for any services it provides. You can configure a computer to use only its local directory domain by using the Directory Access application on the computer.

To restrict a computer to its local directory domain:

- 1 In Directory Access, click the Authentication tab or the Contacts tab.
Click Authentication to configure the search policy used for authentication and most other administrative data.
Click Contacts to configure the search policy used for contact information in some mail, address book, and personal information manager applications.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Choose “Local directory” from the Search pop-up menu, then click Apply.

Changing Basic LDAPv3 Settings

You can use the Directory Access application to change basic settings for accessing LDAPv3 servers, including the shared Open Directory domains of Mac OS X Servers:

- Enable or disable use of LDAPv3 servers supplied by DHCP.
- Reveal an intermediate level of LDAPv3 information and options.

The Open Directory Assistant application also configures use of LDAPv3 servers supplied by DHCP, but does not offer as many options as Directory Access.

Enabling or Disabling Use of DHCP-Supplied LDAPv3 Servers

Your Mac OS X computer can automatically access LDAPv3 servers via DHCP. This automatic access requires that the DHCP service be configured to supply an LDAPv3 server on request.

You can enable or disable this method of accessing an LDAPv3 server for each network location that is defined in the Network pane of System Preferences.

To enable or disable automatic access to an LDAPv3 server:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 From the Location pop-up menu, choose the network location that you want to affect, or use Automatic.
- 5 Click the checkbox to enable or disable use of the LDAPv3 server supplied by DHCP.

If you disable this setting, this computer doesn't use any LDAPv3 servers supplied by DHCP. However, the computer may automatically access shared NetInfo domains. See "Using NetInfo Domains" on page 110 for more information.

If you enable this setting, the DHCP service should be configured to supply one or more LDAPv3 server addresses. For instructions, see "Setting the LDAP Server for DHCP Clients" on page 479 in Chapter 11, "DHCP Service."

Showing or Hiding Available LDAPv3 Configurations

You can show or hide a list of available LDAPv3 server configurations. When you show the list, you see and can change some settings for each LDAPv3 configuration.

To show or hide the available LDAPv3 configurations:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.

- 4 From the Location pop-up menu, choose the network location that you want to see, or use Automatic.
- 5 Click Show Options or Hide Options.

Configuring Access to Existing LDAPv3 Servers

On a Mac OS X computer that is not configured to access an LDAPv3 server automatically via DHCP, you can manually configure access to one or more LDAPv3 servers. You can do the following:

- Create server configurations and enable or disable them individually. For instructions, see “Creating an LDAPv3 Configuration” on page 98.
- Edit the settings of a server configuration. For instructions, see “Editing an LDAPv3 Configuration” on page 99.
- Duplicate a configuration. For instructions, see “Duplicating an LDAPv3 Configuration” on page 99.
- Delete a configuration. For instructions, see “Deleting an LDAPv3 Configuration” on page 100.
- Change the connection settings for an LDAPv3 configuration. For instructions, see “Changing an LDAPv3 Configuration’s Connection Settings” on page 100.
- Define custom mappings of Mac OS X record types and attributes to LDAPv3 record types, search bases, and attributes. For instructions, see “Configuring LDAPv3 Search Bases and Mappings” on page 101.
- Populate LDAPv3 directory domains with records and data. For instructions, see “Populating LDAPv3 Domains With Data for Mac OS X” on page 103.

Creating an LDAPv3 Configuration

You can use Directory Access to create a configuration for an LDAPv3 server.

To create an LDAPv3 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Click New and enter a name for the configuration.
- 6 Press Tab and enter the LDAPv3 server’s DNS name or IP address.
- 7 Choose a mapping template from the inline pop-up menu, or choose From Server.

- 8 Enter the search base for your LDAPv3 server and click OK.

If you chose a template in step 7, you must enter a search base, or the LDAPv3 server will not function.

If you chose From Server in step 7, you may be able to leave the search base blank and have the LDAPv3 server function. In this case, Open Directory will look for the search base at the first level of the LDAPv3 server.

- 9 Select the SSL checkbox if you want Open Directory to use Secure Sockets Layer (SSL) for connections with the LDAPv3 server.

After creating a new server configuration, you should add the server to an automatic search policy supplied by a DHCP server or to a custom search policy. A computer can access an LDAP server only if the server is included in the computer's search policy, either automatic or custom. For more information, see "Setting Up Search Policies" on page 94 and "Setting the LDAP Server for DHCP Clients" on page 479 of Chapter 11, "DHCP Service."

Editing an LDAPv3 Configuration

You can use Directory Access to change the settings of an LDAPv3 server configuration.

To edit an LDAPv3 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Change any of the settings displayed in the list of server configurations.

Click an Enable checkbox to activate or deactivate a server.

To change a configuration name, double-click it in the list.

To change a server name or IP address, double-click it in the list.

Choose a mapping template from the inline pop-up menu.

Click the SSL checkbox to enable or disable Secure Sockets Layer (SSL) connections.

Duplicating an LDAPv3 Configuration

You can use Directory Access to duplicate an LDAPv3 server configuration. After duplicating a configuration, you can change its settings.

To duplicate an LDAPv3 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.

- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Select a server configuration in the list, then click Duplicate.
- 6 Change any of the duplicate configuration's settings.

Click an Enable checkbox to activate or deactivate a server.

To change a configuration name, double-click it in the list.

To change a server name or IP address, double-click it in the list.

Choose a mapping template from the inline pop-up menu.

Click the SSL checkbox to enable or disable Secure Sockets Layer (SSL) connections.

After duplicating a server configuration, you should add the duplicate to an automatic search policy supplied by a DHCP server or to a custom search policy. A computer can access an LDAP server only if the server is included in the computer's search policy, either automatic or custom. For more information, see "Setting Up Search Policies" on page 94 and "Setting the LDAP Server for DHCP Clients" on page 479 of Chapter 11, "DHCP Service."

Deleting an LDAPv3 Configuration

You can use Directory Access to delete an LDAPv3 server configuration.

To delete an LDAPv3 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Select a server configuration in the list, then click Delete.

Changing an LDAPv3 Configuration's Connection Settings

You can use Directory Access to change the connection settings for an LDAPv3 server configuration.

To change the connection settings of an LDAPv3 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Select a server configuration in the list, then click Edit.

- 6 Click the Connection tab and change any of the settings.

Configuration Name identifies this configuration in the list of LDAPv3 configurations. (You can also change the name directly in the list of LDAPv3 configurations.)

Server Name or IP Address specifies the server's DNS name or its IP address. (You can also change this directly in the list of LDAPv3 configurations.)

“Open/close times out in” specifies the number of seconds that Open Directory waits before cancelling an attempt to connect to the LDAPv3 server.

“Connection times out in” specifies the number of seconds that Open Directory allows an idle or unresponsive connection to remain open.

“Use authentication when connecting” determines whether Open Directory authenticates itself as a user of the LDAPv3 server by supplying the Distinguished Name and Password when connecting to the server.

“Encrypt using SSL” determines whether Open Directory encrypts communications with the LDAPv3 server by using Secure Sockets Layer (SSL) connection. (You can also change this setting directly in the list of LDAPv3 configurations.)

“Use custom port” specifies a port number other than the standard port for LDAPv3 connections (389 without SSL or 636 with SSL).

Configuring LDAPv3 Search Bases and Mappings

Each LDAPv3 configuration that you create specifies where data needed by Mac OS X resides on the LDAPv3 server. You can edit the LDAPv3 search base for each Mac OS X record type. You can edit the mapping of each Mac OS X record type to one or more LDAPv3 object classes. For each record type, you can also edit the mapping of Mac OS X data types, or attributes, to LDAPv3 attributes. You edit search bases and mappings with the Directory Access application.

Note: The mapping of Mac OS X data types to LDAPv3 attributes can be different for each record type. Mac OS X has separate LDAPv3 mappings for each record type.

For detailed specifications of record types and attributes required by Mac OS X, see Appendix A, “Open Directory Data Requirements.”

To edit the search bases and mappings for an LDAPv3 server:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Select a server configuration in the list, then click Edit.

6 Click the Search & Mappings tab.

7 Select the mappings that you want to use as a starting point, if any.

Click “Read from Server” to edit the mappings currently stored in the LDAPv3 server whose configuration you are editing.

Click the “Access this LDAPv3 server using” pop-up menu, choose a mapping template to use its mappings as a starting point, or choose Custom to begin with no predefined mappings.

8 Add record types and change their search bases as needed.

To add record types, click the Add button below the Record Types and Attributes list. In the sheet that appears, select Record Types, select one or more record types from the list, and then click OK.

To change the search base of a record type, select it in the Record Types and Attributes List. Then click the “Search base” field and edit the search base.

To remove a record type, select it in the Record Types and Attributes List and click Delete.

To add a mapping for a record type, select the record type in the Record Types and Attributes List. Then click the Add button below “Map to ___ items in list” and enter the name of an object class from the LDAPv3 domain. To add another LDAPv3 object class, you can press Return and enter the name of the object class. Specify whether to use all or any of the listed LDAPv3 object classes by using the pop-up menu above the list.

To change a mapping for a record type, select the record type in the Record Types and Attributes List. Then double-click the LDAPv3 object class that you want to change in the “Map to ___ items in list” and edit it. Specify whether to use all or any of the listed LDAPv3 object classes by using the pop-up menu above the list.

To remove a mapping for a record type, select the record type in the Record Types and Attributes List. Then click the LDAPv3 object class that you want to remove from the “Map to ___ items in list” and click the Delete button below “Map to ___ items in list.”

9 Add attributes and change their mappings as needed.

To add attributes to a record type, select the record type in the Record Types and Attributes List. Then click the Add button below the Record Types and Attributes list. In the sheet that appears, select Attribute Types, select one or more attribute types, and then click OK.

To add a mapping for an attribute, select the attribute in the Record Types and Attributes List. Then click the Add button below “Map to ___ items in list” and enter the name of an attribute type from the LDAPv3 domain. To add another LDAPv3 attribute type, you can press Return and enter the name of the attribute type.

To change a mapping for an attribute, select the attribute in the Record Types and Attributes List. Then double-click the item that you want to change in the “Map to ___ items in list” and edit the item name.

To remove a mapping for an attribute, select the attribute in the Record Types and Attributes List. Then click the item that you want to remove from the “Map to ___ items in list” and click the Delete button below “Map to ___ items in list.”

- 10 Click Write to Server if you want to store the mappings on the LDAPv3 server so that it can supply them automatically to its clients.

You must enter a search base to store the mappings, a distinguished name of an administrator (for example, cn=admin,dc=example,dc=com) and a password.

The LDAPv3 server supplies its mappings to clients that are configured to use an automatic search policy. For instructions on configuring the client search policy, see “Setting Up Search Policies” on page 94.

The LDAPv3 server also supplies its mappings to clients that have been configured manually to get mappings from the server. For instructions on configuring client access to the server, see “Creating an LDAPv3 Configuration” on page 98 through “Changing an LDAPv3 Configuration’s Connection Settings” on page 100.

Populating LDAPv3 Domains With Data for Mac OS X

After configuring LDAPv3 directory domains and setting up their data mapping, you can populate them with records and data for Mac OS X. For directory domains that allow remote administration (read/write access), use the Workgroup Manager application and the Server Settings application as follows:

- Identify share points and shared domains that you want to mount automatically in a user’s /Network directory (the Network globe in Finder windows). Use the Sharing module of Workgroup Manager. For instructions, see Chapter 4, “Sharing.”
- Define users records and group records and configure their settings. Use the Accounts module of Workgroup Manager. For instructions, see Chapter 3, “Users and Groups.”
- Define lists of computers that have the same preference settings and are available to the same users and groups. Use the Computers module of Workgroup Manager. For instructions, see Chapter 6, “Client Management: Mac OS X.”
- Create records for shared printers that you want to appear in the Directory Services printer list in Print Center. Use the Print module of Server Settings. For instructions, see Chapter 7, “Print Service.”

Note: To add records and data to a read-only LDAPv3 domain, you must use tools on the server that hosts the LDAPv3 domain.

Using an Active Directory Server

Your Mac OS X Server, like any computer with Mac OS X version 10.2, can use Open Directory to access an Active Directory domain hosted by a Microsoft Windows server. This section explains how to configure your Mac OS X Server and client Mac OS X computers to access an Active Directory server. This section also explains how to use your Mac OS X Server to populate the Active Directory domain with records and data.

In addition, you can edit, duplicate, or delete an Active Directory server configuration. You can also change the connection settings and customize the mappings of an Active Directory server configuration. The procedures for all these tasks are the same for Active Directory servers as for LDAPv3 servers. For instructions, see “Configuring Access to Existing LDAPv3 Servers” on page 98.

Important Open Directory uses the LDAPv3 protocol, not Microsoft’s proprietary Active Directory Services Interface (ADSI), to connect to Microsoft’s Active Directory. This chapter does not explain how to configure Active Directory on a Windows server for LDAPv3 read/write access. If you need assistance, consult an individual with Windows and Active Directory expertise, refer to the documentation for these products, or go to the Microsoft Web site:

www.microsoft.com/support/

Creating an Active Directory Server Configuration

You can use Directory Access to create a configuration for an Active Directory server.

To create an Active Directory server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv3 in the list of services, then click Configure.
- 4 If the list of server configurations is hidden, click Show Options.
- 5 Click New and enter a name for the configuration.
- 6 Press Tab and enter the Active Directory server’s DNS name or IP address.
- 7 Click the inline pop-up menu and choose Active Directory.
- 8 Enter the search base for your Active Directory server, then click OK.
- 9 Select the SSL checkbox if you want Open Directory to use Secure Sockets Layer (SSL) for connections with the Active Directory server.

After creating a new Active Directory server configuration, you should add the server to an automatic search policy supplied by a DHCP server or to a custom search policy. A computer can access an Active Directory server only if the server is included in the computer's search policy, either automatic or custom. For more information, see "Setting Up Search Policies" on page 94 and "Setting the LDAP Server for DHCP Clients" on page 479 of Chapter 11, "DHCP Service."

Setting Up an Active Directory Server

If you want a Mac OS X computer to get administrative data from an Active Directory server, the data must exist on the Active Directory server in the format required by Mac OS X. You may need to add, modify, or reorganize data on the Active Directory server. You must make the necessary modifications by using tools on the Active Directory server.

To set up an Active Directory server for Mac OS X directory services:

- 1 Go to the Active Directory server and configure it to support LDAPv3-based authentication and password checking.
- 2 Modify the Active Directory object classes and attributes as necessary to provide the data needed by Mac OS X.

For detailed specifications of the data required by Mac OS X directory services, see Appendix A, "Open Directory Data Requirements."

Populating Active Directory Domains With Data for Mac OS X

After creating an Active Directory server configuration and setting it up for Mac OS X directory services, you can populate it with records and data for Mac OS X. If the Active Directory server allows remote administration (read/write access), use the Workgroup Manager application and the Server Settings applications as follows:

- Identify share points and shared domains that you want to mount automatically in a user's /Network directory (the Network globe in Finder windows). Use the Sharing module of Workgroup Manager. For instructions, see Chapter 4, "Sharing."
- Define user records and group records and configure their settings. Use the Accounts module of Workgroup Manager. For instructions, see Chapter 3, "Users and Groups."
- Define lists of computers that have the same preference settings and are available to the same users and groups. Use the Computers module of Workgroup Manager. For instructions, see Chapter 6, "Client Management: Mac OS X."
- Create records for shared printers that you want to appear in the Directory Services printer list in Print Center. Use the Print module of Server Settings. For instructions, see Chapter 7, "Print Service."

Note: To add records and data to a read-only Active Directory server, you must use tools on the Windows server.

Accessing an Existing LDAPv2 Directory

You can configure a Mac OS X computer to retrieve administrative data from one or more LDAPv2 servers. For each LDAPv2 server that you want the computer to access, you generally do the following:

- Prepare the LDAPv2 server data. For instructions, see “Setting Up an LDAPv2 Server” on page 106.
- Create an LDAPv2 server configuration. For instructions, see “Creating an LDAPv2 Server Configuration” on page 106.
- Change LDAPv2 server access settings as needed. For instructions, see “Changing LDAPv2 Server Access Settings” on page 107.
- Edit LDAPv2 search bases and data mappings as needed. For instructions, see “Editing LDAPv2 Search Bases and Data Mappings” on page 108.
- Make sure the LDAPv2 server is included in a custom search policy. For more information, see “Setting Up Search Policies” on page 94.

Setting Up an LDAPv2 Server

If you want a Mac OS X computer to get administrative data from an LDAPv2 server, the data must exist on the LDAPv2 server in the format required by Mac OS X. You may need to add, modify, or reorganize data on the LDAPv2 server. Mac OS X cannot write data to an LDAPv2 directory, so you must make the necessary modifications by using tools on the server that hosts the LDAPv2 directory.

To set up an LDAPv2 server for Mac OS X:

- 1 Go to the LDAPv2 server and configure it to support LDAPv2-based authentication and password checking.
- 2 Modify LDAPv2 server object classes and attributes as necessary to provide the data needed by Mac OS X.

For detailed specifications of the data required by Mac OS X directory services, see Appendix A, “Open Directory Data Requirements.”

Creating an LDAPv2 Server Configuration

You need to create a configuration for an LDAPv2 server from which you want your computer to get administrative data. Use the Directory Access application to create an LDAPv2 configuration.

To create an LDAPv2 server configuration:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.

- 3 Select LDAPv2 in the list of services, then click Configure.
- 4 Create a new configuration or duplicate an existing configuration.
Click New to create a new configuration.
Click Duplicate to create a copy of the currently selected configuration.
- 5 Click the Identity tab, then enter a configuration name and server address.
In the Name field, enter a descriptive name for the LDAPv2 server.
In the Address field, enter the LDAPv2 server's DNS name or IP address.
- 6 Click the Access tab, then change the access settings as needed.
For detailed instructions, see “Changing LDAPv2 Server Access Settings” on page 107.
- 7 Click the Records tab and for any Mac OS X record type listed on the left, edit the LDAPv2 search base as needed on the right.
For detailed instructions, see “Editing LDAPv2 Search Bases and Data Mappings” on page 108.
- 8 Click the Data tab and for any Mac OS X data type listed on the left, edit the corresponding LDAPv2 attributes on the right.
For detailed instructions, see “Editing LDAPv2 Search Bases and Data Mappings” on page 108.
- 9 Click OK.
- 10 Select the Enable checkbox to make the LDAPv2 server you just configured available for use by directory services, then close the window and click Save.

After creating a new LDAPv2 server configuration, you should add the server to a custom search policy. A computer can access an LDAPv2 server only if the server is included in the computer's custom search policy. For more information, see “Setting Up Search Policies” on page 94 and “Setting the LDAP Server for DHCP Clients” on page 479 of Chapter 11, “DHCP Service.”

Changing LDAPv2 Server Access Settings

You can change settings that determine how your computer accesses an LDAPv2 server. Use the Directory Access application to change the settings.

To change access settings for an LDAPv2 server:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv2 in the list of services, then click Configure.
- 4 Select a server configuration in the list, then click Edit.
- 5 Click the Access tab, then change the access settings as needed.

Select “Use anonymous access” if Open Directory should connect to the LDAPv2 server without using a name and password.

Select “Use the username and password below” if Open Directory should not connect anonymously. Enter the distinguished name (for example, cn=admin, cn=users, dc=example, dc=com) and password that Open Directory should use to establish an LDAPv2 server connection. Ensure that the LDAPv2 server is configured to accept any name and password you specify.

Enter the number of seconds for “Open & close timeout,” which defines the maximum time to wait before cancelling an attempt to connect to the LDAPv2 server. The default is 120 seconds.

Enter the number of seconds for “Search timeout,” which defines the maximum time to spend searching for data on the LDAPv2 server. The default is 120 seconds.

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 LDAPv2 server.

- 6 Click OK, then close the window and click Save.

Editing LDAPv2 Search Bases and Data Mappings

Each LDAPv2 configuration that you create specifies where data needed by Mac OS X resides on the LDAPv2 server. You can edit the LDAPv2 search base for each Mac OS X record type. You can also edit the mapping of Mac OS X data types, or attributes, to LDAPv2 attributes. You edit search bases and data mappings with the Data Access application.

Note: The mapping of Mac OS X data types to LDAPv2 attributes is the same for all record types. Mac OS X cannot have different LDAPv2 mappings for different record types.

For detailed specifications of record types and attributes required by Mac OS X, see Appendix A, “Open Directory Data Requirements.”

To edit the search bases and data mappings for an LDAPv2 server:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select LDAPv2 in the list of services, then click Configure.
- 4 Select a server configuration in the list, then click Edit.
- 5 Click the Records tab and for any Mac OS X record type listed on the left, edit the LDAPv2 search base as needed on the right.

Select an item in the Record Type list, and then edit the “Maps to” value to specify a search base on the LDAPv2 server that provides appropriate information.

Select Users in the Record Type list. Then edit the “Maps to” value to specify a search base on the LDAPv2 server that provides user information. The default search base for the Users record type is ou=people, o=company name.

Select Groups in the Record Type list. Then edit the “Maps to” value to specify a search base on the LDAPv2 server that provides group information. The default search base for the Groups record type is ou=groups, o=company name.

As needed, select other items in the Record Types list and edit their “Maps to” values to specify a search base on the LDAPv2 server that specifies the appropriate information.

- 6 Click the Data tab and for any Mac OS X data type listed on the left, edit the corresponding LDAPv2 attributes on the right.

Select RecordName in the Data Type column. Then edit the “Maps to” value to identify one or more LDAPv2 attributes that store the names a user can be known by, including the user’s short name. This same mapping identifies the LDAPv2 attributes that store a group name for the Groups record type.

Select UniqueID in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attribute that uniquely identifies a user. This same mapping identifies the LDAPv2 attribute that uniquely identifies a group in the Groups record type.

Select RealName in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores the full user name.

Select MailAttribute in the Data Type column if users will be using mail service on the server. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores the user’s mail settings in the required format.

Select EMailAddress in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attributes that store the forwarding address. This attribute is used for users without a mail attribute.

Select Password in the Data Type column only if the LDAPv2 server stores user passwords in UNIX crypt format. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores the password.

Select PrimaryGroupID in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores the ID number for the user’s primary group.

Select HomeDirectory in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attributes that store the home directory information in the required format.

Select UserShell in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores the path and filename of the user login shell. This is the default shell used for command-line interactions with the server. Enter “None” to prevent users who are defined in this directory from accessing the server remotely via a command line.

Select GroupMembership in the Data Type column. Then edit the “Maps to” value to identify the LDAPv2 attribute that stores a list of users associated with the group. Users should be identified using their short names.

If other items in the Data Type column will be retrieved from the LDAPv2 server, select them one by one. When you select an item, edit the “Maps to” value to identify one or more LDAPv2 attributes that store the appropriate information.

- 7 Click OK, then close the window and click Save.

Using NetInfo Domains

Your Mac OS X Server can be part of a hierarchy of shared NetInfo domains. If you create a shared directory domain on your server, other Mac OS X computers can access it via the NetInfo protocol (as well as the LDAPv3 protocol). This makes your server a NetInfo parent, and the other computers that bind to it are NetInfo children. Instructions for creating a shared NetInfo domain are next.

You can also configure your Mac OS X Server to bind to a shared NetInfo domain on another Mac OS X Server. This makes your server a NetInfo child of a NetInfo parent. For instructions, see “Configuring NetInfo Binding” on page 111.

Expert system administrators can manage NetInfo domains as follows:

- Create machine records for broadcast binding to a shared NetInfo domain. For instructions, see “Adding a Machine Record to a Parent NetInfo Domain” on page 113.
- Configure a shared NetInfo domain to use a particular port number instead of a dynamically assigned port number. For instructions, see “Configuring Static Ports for Shared NetInfo Domains” on page 113.
- View the contents of any NetInfo domain. For instructions, see “Viewing and Changing NetInfo Data” on page 114.
- Perform other operations by using the Terminal application. For more information, see “Using UNIX Utilities for NetInfo” on page 114.

Creating a Shared NetInfo Domain

Your Mac OS X Server can host a shared NetInfo domain. Then other Mac OS computers can access the shared NetInfo domain for information about users and resources. The server that hosts a shared NetInfo domain is called a *parent*, and a computer that accesses it is known as a *child*.

The shared domain is actually a shared Open Directory domain that other computers access using the NetInfo protocol. You set it up with the Open Directory Assistant application.

To create a shared NetInfo domain:

- 1** Open the Open Directory Assistant application.
- 2** Enter the connection and authentication information for the Mac OS X Server where you want to create the shared NetInfo domain, then click Connect.
- 3** Click the right arrow to get to the Location step, and then select the setting that indicates the server is at its permanent network location.

You cannot set up a shared NetInfo domain on a server that is in a temporary location.

- 4** Advance to the Directory Use step, and then select the option to provide directory information to other servers.
- 5** Go to the Configure step, where you may select the option to enable LDAP support.

The shared directory automatically supports the NetInfo protocol. LDAP support is optional.

- 6** Go through the steps for configuring a Password Server.

As you go through each step, Open Directory Assistant displays the current Password Server settings of the Mac OS X Server that you are configuring.

If you want the Password Server configuration to remain as-is, do not change any settings as you go through these steps.

- 7** When you reach the Finish Up step, review its configuration summary and click Go Ahead to apply the settings.

If you want to change any of the settings in the configuration summary, click the left arrow. Keep clicking the left arrow until you get back to the step where you can make the desired change. After changing the setting, click the right arrow until you get to the Finish Up step again.

Configuring NetInfo Binding

When a Mac OS X computer starts up, it can bind its local directory domain to a shared NetInfo domain. The shared NetInfo domain can bind to another shared NetInfo domain. The binding process creates a hierarchy of NetInfo domains.

A NetInfo hierarchy has a structure like an upside-down tree. Local domains at the bottom of the hierarchy bind to one or more shared domains, which may in turn bind to one or more other shared domains, and so on. Each domain binds to only one shared domain, but a shared domain can have any number of domains bind to it. A shared domain is called parent domain, and each domain that binds to it is a child domain. At the top of the hierarchy is one shared domain that doesn't bind to another domain; this is the *root* domain.

A Mac OS X computer can bind to a shared NetInfo domain by using any combination of three protocols: static, broadcast, or DHCP.

- With static binding, you specify the address and NetInfo tag of the shared NetInfo domain. This is most commonly used when the shared domain's computer is not on the same IP subnet as the computer that needs to access it.
- With DHCP binding, a DHCP server automatically supplies the address and NetInfo tag of the shared NetInfo domain. To use DHCP binding, the DHCP server must be configured to supply a NetInfo parent's address and tag. For instructions, see "Setting NetInfo Options for a Subnet" on page 482 in Chapter 11, "DHCP Service."
- With broadcast binding, the computer locates a shared NetInfo domain by sending out an IP broadcast request. The computer hosting the shared domain responds with its address and tag.

For broadcast binding, both computers must be on the same IP subnet or on a network that is configured for IP broadcast forwarding.

The parent domain must have the NetInfo tag "network."

The parent domain must have a machine record for each of its child domains. See "Adding a Machine Record to a Parent NetInfo Domain" on page 113 for more information.

If you configure a computer to use multiple binding protocols and a parent is not located with one protocol, another one is used. The protocols are used in this order: static, DHCP, broadcast.

You can configure NetInfo binding by using the Directory Access application.

To bind a Mac OS X computer to a shared NetInfo domain:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select NetInfo in the list of services, then click Configure.
- 4 Select the binding protocols that you want the computer to use.

For broadcast binding, select "Attempt to connect using Broadcast protocol."

For DHCP binding, select "Attempt to connect using DHCP protocol."

For static binding, select "Attempt to connect to a specific NetInfo server." Then enter the IP address of the parent domain's computer in the Server Address field and the parent domain's NetInfo tag in the Server Tag field.

- 5 Click OK, then click Apply.
- 6 Restart the computer.

Adding a Machine Record to a Parent NetInfo Domain

Mac OS X computers can bind their directory domains to a parent NetInfo domain by using broadcast binding. The parent NetInfo domain must have a machine record for each Mac OS X computer that can bind to it with broadcast binding. You can create a machine record with the NetInfo Manager application.

To add a machine record to a parent NetInfo domain:

- 1 Open NetInfo Manager on the computer where the parent domain resides, then open the domain.
- 2 Click the lock and log in using the user name and password specified when the domain was created.
- 3 Select the machines directory in the Directory Browser list.
- 4 Choose New Subdirectory from the Directory menu,.
- 5 Double-click new_directory in the lower list and enter the DNS name of the child computer.
- 6 Choose New Property from the Directory menu.
- 7 In the lower list, change new_property to ip_address and change new_value to the IP address of the child computer.
- 8 Choose New Property from the Directory menu.
- 9 Change new_property to “serves” and then change new_value to the name and NetInfo tag of the child’s local domain, using a “/” to separate them.

For example, you would change new_value to marketing.demo/local for the local domain of the computer named marketing.demo.
- 10 Choose Save Changes from the Domain menu, then click Update This Copy.

Configuring Static Ports for Shared NetInfo Domains

By default, Mac OS X dynamically selects a port in the range 600 through 1023 when it accesses a shared NetInfo domain. You can configure a shared domain for NetInfo access over specific ports. Use the NetInfo Manager application to do this.

To configure specific ports for NetInfo access to shared domains:

- 1 Open NetInfo Manager on the computer where the shared domain resides, then open the domain.
- 2 Click the lock icon and log in using the administrator name and password specified when the domain was created.
- 3 Select the “/” directory in the Directory Browser list.
- 4 To change the value of an existing port property, double-click the value in the Value(s) column and make the change.

- 5 To delete a port property, select it and choose Delete from the Edit menu.
- 6 To add a property, choose New Property from the Directory menu and proceed as follows.

If you want to use one port for both TCP and UDP packets, double-click new_property and change it to port. Then change new_value to the port number you want to use.

If you want separate TCP and UDP ports, double-click new_property and change it to tcp_port. Then change new_value to the TCP port number you want to use. Next double-click new_property and change it to udp_port. This time, change new_value to the UDP port number you want to use.

Viewing and Changing NetInfo Data

Information in a NetInfo database is organized into directories, which are specific categories of NetInfo records, such as users, machines, and mounts. For example, the users directory contains a record for each user defined in the domain.

Each record is a collection of properties. Each property has a key (listed in the Property column) and one or more values (shown in the Value(s) column). The key is used by processes to retrieve values.

The user named “root” in a domain can change any of its properties or add new ones. Properties with the prefix “_writers_” list the short names of other users authorized to change the value of a particular property. For example, _writers_passwd is the short name of the user who can change this user’s password.

You can use NetInfo Manager, located in /Applications/Utilities, on any Mac OS X computer to view the administrative data in a NetInfo domain.

Using UNIX Utilities for NetInfo

Several UNIX command-line utilities that interact with NetInfo are available through the Terminal application. To find out more about these utilities, view their man pages.

Utility	Description
niload	Loads data from UNIX configuration files (such as /etc/passwd) into a NetInfo database.
nidump	Converts data from a NetInfo database to a UNIX configuration file.
niutil	Reads from a NetInfo database and writes to one.
nigrep	Searches all NetInfo domains for all instances of a string you specify.
niel	Creates, reads, or manages NetInfo data.

Using Berkeley Software Distribution (BSD) Configuration Files

Historically, UNIX computers have stored administrative data in configuration files such as

`/etc/passwd`

`/etc/group`

`/etc/hosts`

Mac OS X is based on a BSD version of UNIX, but normally gets administrative data from directory domains for the reasons discussed at the beginning of this chapter.

In Mac OS X version 10.2 and later (including Mac OS X Server version 10.2 and later), Open Directory can retrieve administrative data from BSD configuration files. This capability enables organizations that already have BSD configuration files to use copies of the existing files on Mac OS X computers. BSD configuration files can be used alone or in conjunction with other directory domains.

To use BSD configuration files, you must do the following:

- Specify which BSD configuration files to use, and map their contents to Mac OS X record types and attributes. Instructions for doing this are next.
- Set up each BSD configuration file with the data required by Mac OS X directory services. See “Setting Up Data in BSD Configuration Files” on page 118 for instructions.
- Create a custom search policy that includes the BSD configuration files domain. For instructions, see “Defining a Custom Search Policy” on page 95.

Mapping BSD Configuration Files

A computer with Mac OS X version 10.2 or later can get information about users and resources from BSD configuration files. Mac OS X determines which BSD configuration files to use by inspecting the file `DSFFPlugin.plist` (located in `/Library/Preferences/DirectoryService/`). This file identifies each BSD configuration file that contains administrative data. In addition, `DSFFPlugin.plist` maps the data in each BSD configuration file to specific Mac OS X record types and attributes. In other words, `DSFFPlugin.plist` tells Mac OS X how to extract particular data items from BSD configuration files.

The `DSFFPlugin.plist` file initially specifies four BSD configuration files for administrative data:

`/etc/master.passwd`

`/etc/group`

`/etc/hosts`

`/etc/fstab`

You can specify different BSD configuration files by editing the DSFFPlugin.plist file. This file contains structured text in XML format and is known as a *property list* or *plist*. You can edit this file with a text editor, but the Property List Editor application makes the job easier. Property List Editor is specifically designed to work with plist files.

You may not have Property List Editor on your computer, because it is not part of a standard installation of Mac OS X. However, Property List Editor is included if you install the Mac OS X Developer Tools from the Developer Tools CD. (The Developer Tools CD comes with the Mac OS X CD.) Then Property List Editor is located in /Developer/Applications.

You can use Directory Access to open the DSFFPlugin.plist file with Property List Editor.

Note: To use the files specified by DSFFPlugin.plist, a computer must have a custom search policy that includes the BSD configuration files domain. An automatic search policy does not include the BSD configuration files domain. See “Defining a Custom Search Policy” on page 95 for instructions.

To map BSD configuration files to Mac OS X record types and attributes:

- 1 In Directory Access, click the Services tab.
- 2 If the lock icon is locked, click it and type the name and password of a server administrator.
- 3 Select BSD Configuration Files in the list of services, then click Configure.

Directory Access tells Property List Editor to open /Library/Preferences/DirectoryService/DSFFPlugin.plist.

- 4 With DSFFPlugin.plist open in Property List Editor, click disclosure triangles in the Property List column to see the contents of FileTypeArray.

FileTypeArray contains dictionary items. Each dictionary identifies one BSD configuration file and maps its contents. Each dictionary is identified by a number. Initially, dictionary 0 maps data in the /etc/hosts file; dictionary 1 maps data in the /etc/group file; dictionary 2 maps data in the /etc/master.passwd file, and directory 3 maps to data in the /etc/fstab file.

- 5 To include another BSD configuration file, add a new dictionary under FileTypeArray and add fields under the new dictionary to specify the file name and path, record type, attributes, and so on.

Add a dictionary for another BSD configuration file by selecting FileTypeArray and clicking New Child. Then click the class of the new dictionary and choose Dictionary from the pop-up menu.

Add a field under a dictionary by selecting the dictionary, clicking its disclosure triangle so it points down, and clicking New Child. Type a name for the field. Then click the class of the field and select the appropriate class from the pop-up menu. Next, change the field's value as needed.

The dictionary that defines a BSD configuration file has the fields specified in the table below. You can see examples of these fields in the preconfigured dictionaries for /etc/hosts, /etc/group, /etc/master.passwd, and /etc/fstab. For detailed specifications of the data required by Mac OS X directory services, see Appendix A, “Open Directory Data Requirements.”

- 6 If necessary, you can delete any line, including a dictionary line, by selecting the line and clicking Delete.

If you delete a line by mistake, immediately choose Undo from the Edit menu.

- 7 When you finish, save and close the file.

Field name	Purpose
AlternateRecordNameIndex (optional)	An index that can be used as a second field to be searched as the record name
CommentChar (optional)	A string that contains the hexadecimal ASCII code of a character to be used to denote comment lines. This character must appear at the beginning of any line that is to be interpreted as a comment. Typically this character is # (hexadecimal 23)
FieldDelimiter	A string that contains the hexadecimal ASCII code of a character to be used to delimit each field within a record. Typically this character is a colon (hexadecimal 3A)
FieldNamesAndPositions	An array of dictionaries. Each dictionary is one field within the record. Each dictionary contains the FieldName and its position (zero based) within the record. The field names must be Mac OS X directory services attributes such as dsAttrTypeStandard:RecordName
FilePath	The path to the BSD configuration file
NumberOfFields	Specifies how many fields are in each record
PasswordArrayIndex (optional)	Specifies which field in each record contains the password
RecordDelimiter	Specifies the hexadecimal ASCII codes of up to eight characters used to delimit the end of a record. Typically this is the newline character (hexadecimal 0A).
RecordNameIndex	An index of the field to be used as the record name

Field name	Purpose
RecordType	The directory services record type of this record
ValueDelimiter (optional)	A string that contains the hexadecimal ASCII code of a character to be used to delimit values within a multivalued field. Typically this is a comma (hexadecimal 2C).

Setting Up Data in BSD Configuration Files

If you want a Mac OS X computer to get administrative data from BSD configuration files, the data must exist in the files and must be in the format required by Mac OS X. You may need to add, modify, or reorganize data in the files. Mac OS X cannot write data to BSD configuration files, so you must make the necessary modifications by using a text editor or other tools.

For detailed specifications of the data required by Mac OS X directory services, see Appendix A, “Open Directory Data Requirements.”

Configuring Directory Access on a Remote Computer

You can use the Directory Access application to configure a computer that uses Mac OS X version 10.2 or later. Remote configuration is initially disabled on Mac OS X client computers and is initially enabled on Mac OS X Servers.

Note: Apple recommends that remote configuration never be disabled on a Mac OS X Server.

To configure directory access on a remote computer:

- 1 Make sure the remote computer has remote access enabled.
On the remote computer, open Directory Access. If its Server menu includes Enable Remote Configuration, choose this item.
- 2 In Directory Access on your computer, choose Connect from the Server menu.
- 3 Enter the connection and authentication information for the computer that you want to configure, then click Connect.
For Address, enter the DNS name or IP address of the server that you want to configure.
For User Name, enter the user name of an administrator on the server.
For Password, enter the password for the user name you entered.
- 4 Click the Services, Authentication, and Contacts tabs and change settings as needed.
All the changes you make affect the remote computer to which you connected in the foregoing steps.

- 5 When you finish configuring the remote computer, choose Disconnect from the Server menu on your computer.

Monitoring Directory Services

You can use the Server Status application to view directory service status and directory service logs. The following logs are available:

- Local directory client log
- LDAP server log
- NetInfo server log

To see directory services status or logs:

- 1 In Server Status, select Directory Servers in the Devices & Services list.
- 2 Click the Overview tab to see status information.
- 3 Click the Logs tab and choose a log from the Show pop-up menu.

Backing Up and Restoring Directory Services Files

You can back up the following directory services data:

- *Open Directory domain data:* Information associated with Open Directory domains is stored in files that reside in `/var/db/netinfo/`. Back up the entire directory.
- *Authentication Manager for Windows data:* If you upgraded your Mac OS X Server from an earlier version and enabled the Authentication Manager for Windows clients before upgrading, 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`. After restoring the domain, restore the corresponding `.tim` file to ensure proper authentication for Windows users who are configured to use Authentication Manager.
- *Directory services configuration:* Configurations set up using the Directory Access application are stored in `/Library/Preferences/DirectoryService/`. Back up the entire directory.

Before backing up this data, quit Directory Access.

Users and Groups

User and group accounts play a fundamental role in a server's day-to-day operations:

- A *user account* stores data Mac OS X Server needs to validate a user's identity and provide services for the user, such as access to particular files on the server and preferences that various services use.
- A *group account* offers a simple way to manage a collection of users with similar needs. A group account stores the identities of users who belong to the group as well as information that lets you customize the working environment for members of a group.

This chapter begins by highlighting the main characteristics of user and group accounts, then goes on to summarize the aspects of account administration and tell you how to

- manage user accounts
- manage home directories
- manage group accounts
- find user and group accounts defined on your network
- use Workgroup Manager shortcuts for defining users and groups
- import user and group accounts from a file
- set up a password validation scheme for each user

Most of the information in this chapter does not require extensive server administration or UNIX experience, but here are several suggestions for server administrators:

- An understanding of Mac OS X Server's directory service options is very useful for working with user and group accounts in different kinds of directory domains and for creating and using Password Servers. Chapter 2, "Directory Services," provides conceptual information as well as directory domain and Password Server setup instructions.
- The `dsimportexport` tool information may be easier to understand if you have experience with command-line tools.
- Kerberos information presumes a working familiarity with Kerberos.

How User Accounts Are Used

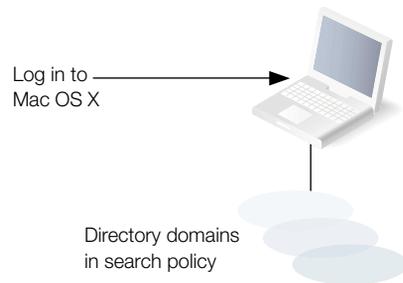
When you define a user's account, you specify the information needed to prove the user's identity: user name, password, and user ID. Other information in a user's account is needed by various services—to determine what the user is authorized to do and perhaps to personalize the user's environment.

Authentication

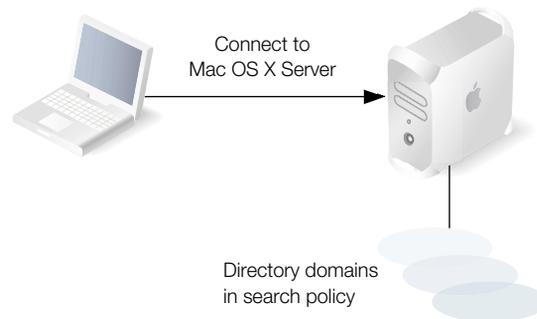
Before a user can log in to or connect with a Mac OS X computer, he or she must enter a name and password associated with a user account that the computer can find.

A Mac OS X computer can find user accounts that are stored in a directory domain of the computer's search policy. A *directory domain* is like a database that a computer is configured to access in order to retrieve configuration information. A *search policy* is a list of directory domains the computer searches when it needs configuration information, starting with the local directory domain on the user's computer. Chapter 2, "Directory Services," describes the different kinds of directory domains and tells you how to configure search policies on any Mac OS X computer.

In the following picture, for example, a user logs in to a Mac OS X computer that can locate the user's account in a directory domain of its search policy.



After login, the user can connect to a remote Mac OS X computer if the user's account can be located within the search policy of the remote computer



If Mac OS X finds a user account containing the name entered by the user, it attempts to validate the password associated with the account. If the password can be validated, the user is authenticated and the login or connection process is completed.

After logging in to a Mac OS X computer, a user has access to all the resources, such as printers and share points, defined in directory domains of the search policy set up for the user's computer. A *share point* is a hard disk (or hard disk partition), CD-ROM disc, or folder that contains files you want users to share. The user can access his home directory by clicking Home in a Finder window or in the Finder's Go menu.

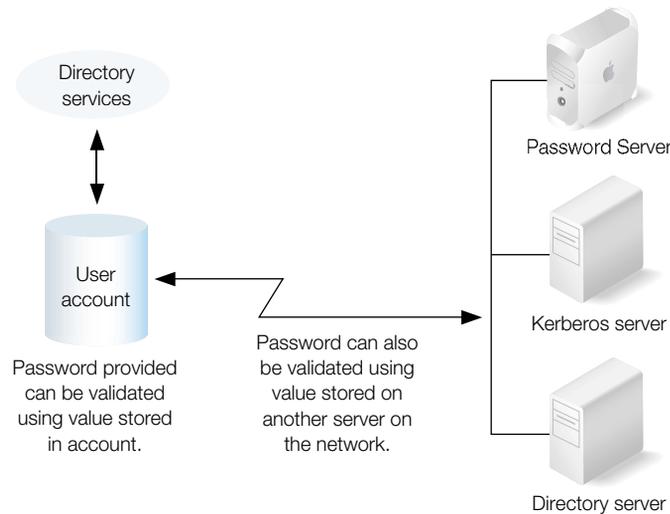
A user does not have to log in to a server to gain access to resources on a network, however. For example, when a user *connects to* a Mac OS X computer, the user can access files he or she is authorized to access on the computer, although the file system may prompt the user to enter a user name and password first. When a user accesses a server's resources without logging in to the server, the search policy of the *user's* computer is still in force, not the search policy of the computer the user has connected with.

Password Validation

When authenticating a user, Mac OS X first locates the user's account and then uses the password strategy designated in the user's account to validate the user's password. There are several password strategies from which to choose:

- The password a user provides can be validated using a value stored in the user's account. The account can be stored in a server-resident directory domain or in a directory domain that resides on another vendor's directory server, such as an LDAP or Active Directory server.
- The password a user provides can be validated using a value stored in an Open Directory Password Server
- A Kerberos server can be used to validate the password.

- A non-Apple LDAP server can be used to validate the password.



Clients needing password validation, such as login window and the AFP server, call Mac OS X directory services. Directory services determine from the user's account how to validate the password.

- Directory services can validate a password stored in the account or by interacting with the Password Server or a remote LDAP directory server (using LDAP bind authentication).
- If a Kerberos server is used to validate a user, when the user accesses a Kerberized client, such as Mac OS X AFP or mail, the client interacts directly with the Kerberos server to validate the user. Then the client interacts with directory services to retrieve the user's record for other information it needs, such as the user ID (UID) or primary group ID.

Information Access Control

All directories (folders) and files on Mac OS X computers have access privileges for the file's owner, a group, and everyone else.



Owner 127 can: Read & Write
 Group 2017 can: Read only
 Everyone else can: None

Mac OS X uses a particular data item in a user's account—the UID—to keep track of directory and file access privileges.

Directory and File Owner Access

When a directory or file is created, the file system stores the UID of the user who created it. When a user with that UID accesses the directory or file, he or she has read and write privileges to it by default. In addition, any process started by the creator has read and write privileges to any files associated with the creator's UID.

If you change a user's UID, the user may no longer be able to modify or even access files and directories he or she created. Likewise, if the user logs in as a user whose UID is different from the UID he or she used to create the files and directories, the user will no longer have owner access privileges for them.

Directory and File Access by Other Users

The UID, in conjunction with a group ID, is also used to control access by users who are members of particular groups.

Every user belongs to a primary group. The primary group ID for a user is stored in his user account. When a user accesses a directory or file and the user is not the owner, the file system checks the file's group privileges.

- If the user's primary group ID matches the ID of the group associated with the file, the user inherits group access privileges.
- If the user's primary group ID does not match the file's group ID, Mac OS X searches for the group account that does have access privileges. The group account contains a list of the short names of users who are members of the group. The file system maps each short name in the group account to a UID, and if the user's UID matches a UID of a group member, the user is granted group access privileges for the directory or file.

Administration Privileges

A user's administrator privileges are stored in the user's account. Administrator privileges determine the extent to which the user can view information about or change the settings of a particular Mac OS X Server or a particular directory domain residing on Mac OS X Server.

Server Administration

Server administration privileges control the powers a user has when logged in to a particular Mac OS X Server. For example:

- A user who is a server administrator can use Server Status and can make changes to a server's search policy using Directory Access.
- A server administrator can see *all* the AFP directories on the server, not just share points.

When you assign server administration privileges to a user, the user is added to the group named "admin" in the local directory domain of the server. Many Mac OS X applications—such as Server Status, Directory Access, and System Preferences—use the admin group to determine whether a particular user can perform certain activities with the application.

Local Mac OS X Computer Administration

Any user who belongs to the group “admin” in the local directory domain of *any* Mac OS X computer has administrator rights on that computer.

Directory Domain Administration

When you want certain users to be able to use Workgroup Manager to manage only certain user, group, and computer accounts residing in Apple’s directory domains, you can make them directory domain administrators. For example, you may want to make a network administrator the server administrator for all your classroom servers, but give individual teachers the privileges to manage student accounts in particular directory domains.

Any user who has a user account in a directory domain can be made an administrator of that domain.

You can control the extent to which a directory domain administrator can change account data stored in a domain. For example, you may want to set up directory domain privileges so that your network administrator can add and remove user accounts, but other users can change the information for particular users. Or you may want different users to be able to manage different groups.

When you assign directory domain administration privileges to a user, the user is added to the admin group of the server on which the directory domain resides.

Home Directories

The location of a user’s home directory is stored in the user account. A *home directory* is a folder where a user’s files and preferences are stored. Other users can see a user’s home directory and read files in its Public folder, but they can’t (by default) access anything else in that directory.

When you create a user in a directory domain on the network, you specify the location of the user’s home directory on the network, and the location is stored in the user account and used by various services, including the login window and Mac OS X managed user services. Here are several examples of activities that use the location of the home directory:

- A user’s home directory is displayed when the user clicks Home in a Finder window or chooses Home from the Finder’s Go menu.
- Home directories that are set up for mounting automatically in a network location, such as /Network/Servers, appear in the Finder on the computer where the user logs in.
- System preferences and managed user settings for Mac OS X users are retrieved from their home directories and used to set up their working environments when they log in.

Mail Settings

You can create a Mac OS X Server mail service account for a user by setting up mail settings in the user's account. To use the mail account, the user simply configures a mail client using the user name, password, mail service, and mail protocol you specify in the mail settings.

Mail account settings let you enable and disable the user's access to mail services running on a particular Mac OS X Server. You can also manage such account characteristics as how to handle automatic message arrival notification.

Settings for Mac OS X mail service are configured using Server Settings, as Chapter 9, "Mail Service," describes.

Resource Usage

Disk, print, and mail quotas can be stored in a user account.

Mail and disk quotas limit the number of megabytes a user can use for mail or files.

Print quotas limit the number of pages a user can print using Mac OS X Server print services. Print quotas also can be used to disable a user's print service access altogether. User print settings work in conjunction with print server settings, which are explained in "Enforcing Quotas for a Print Queue" on page 322.

User Preferences

Any preferences you define for a Mac OS X user are stored in the user's account. Preferences you define for Mac OS 8 and 9 users are stored using Macintosh Manager. See Chapter 6, "Client Management: Mac OS X," and Chapter 10, "Client Management: Mac OS 9 and OS 8," for information about user preferences.

How Group Accounts Are Used

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 Mac OS X Server.

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

Information Access Control

Information in group accounts is used to help control user access to directories and files. See "Directory and File Access by Other Users" on page 125 for a description of how this works.

Group Directories

When you define a group, you can also specify a directory for storing files you want group members to share. The location of the directory is stored in the group account.

You can grant administration privileges for a group directory to a user. A group directory administrator has owner privileges for the group directory and can use the Finder to change group directory attributes.

Workgroups

When you define preferences for a group it is known as a workgroup. A *workgroup* provides you with a way to manage the working environment of group members.

Any preferences you define for a Mac OS X workgroup are stored in the group account. Preferences for Mac OS 8 and 9 workgroups are stored using Macintosh Manager. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for a description of workgroup preferences.

Computer Access

You can set up computer accounts, which let you restrict access to particular computers by members of specific groups. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for a description of how to set up computer accounts and specify preferences for them.

Kinds of Users and Groups

Mac OS X Server uses several different kinds of users and groups. Most of these are user-defined—user and group accounts that you create. There are also some pre-defined user and group accounts, which are reserved for use by Mac OS X.

Users and Managed Users

Depending on how you have your server and your user accounts set up, users can log in using Mac OS 8, 9, and X computers; Windows computers; or UNIX computers—stationary or portable—and be supported by Mac OS X Server in their work.

Most users have an individual account, which is used to authenticate them and control their access to services. When you want to personalize a user’s environment, you define user, group, and/or computer preferences for the user. Sometimes the term “managed client” or “managed user” is used for a user who has preferences associated with his account. “Managed client” is also used to refer to computer accounts that have preferences defined for them.

When a managed user logs in, the preferences that take effect are a combination of his user preferences and preferences set up for any workgroup or computer list he or she belongs to. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for managed user information.

Groups, Primary Groups, and Workgroups

As noted earlier, when you define preferences for a group, the group is known as a *workgroup*.

A *primary group* is the user’s default group. As “Directory and File Access by Other Users” on page 125 describes, primary groups can expedite the checking done by the Mac OS X file system when a user accesses a file.

Administrators

Users with server or directory domain administration privileges are known as *administrators*. Administrators are always members of the predefined “admin” group.

Guest Users

Sometimes you want to provide services for individuals who are anonymous—that is, they can’t be authenticated because they don’t have a valid user name or password. These users are known as *guest users*.

Some services, such as AFP, let you indicate whether you want to let guest users access files. If you enable guest access, users who connect anonymously are restricted to files and folders with privileges set to Everyone.

Another kind of guest user is a managed user that you can define to allow easy setup of public computers or kiosk computers. See Chapter 10, “Client Management: Mac OS 9 and OS 8,” for more about these kinds of users.

Predefined Accounts

The following table describes the user accounts that are created automatically when you install Mac OS X (unless otherwise indicated).

Predefined user name	Short name	UID	Use
Anonymous FTP User	ftp	98	The user name given to anyone using FTP as an anonymous user. This user is created the first time the FTP server is accessed if the FTP server is turned on, if anonymous FTP access is enabled, and if the anonymous-ftp user does not already exist.
Macintosh Manager User	mmuser	-17	The user created by Macintosh Management Server when it is first started on a particular server. It has no home directory, and its password is changed periodically.
System Administrator	root	0	The most powerful user.
System Services	daemon	1	A legacy UNIX user.
Sendmail User	smmsp	25	The user that sendmail runs as.
Unknown User	unknown	99	The user that is used when the system doesn't know about the hard drive.
Unprivileged User	nobody	-2	This user was originally created so that system services don't have to run as System Administrator. Now, however, service-specific users, such as World Wide Web Server, are often used for this purpose.
World Wide Web Server	www	70	The nonprivileged user that Apache uses for its processes that handle requests.
My SQL Server	mysql	74	The user that the MySQL database server uses for its processes that handle requests.

The following table characterizes the group accounts that are created automatically when you install Mac OS X.

Predefined group name	Group ID	Use
admin	80	The group to which users with administrator privileges belong.
bin	7	A group that owns all binary files.
daemon	1	A group used by system services.
dialer	68	A group for controlling access to modems on a server.
guest	31	
kmem	2	A legacy group used to control access to reading kernel memory.
mail	6	The group historically used for access to local UNIX mail.
mysql	74	The group that the MySQL database server uses for its processes that handle requests.
network	69	This group has no specific meaning.
nobody	-2	A group used by system services.
nogroup	-1	A group used by system services.
operator	5	This group has no specific meaning.
smmsp	25	The group used by sendmail.
staff	20	The default group into which UNIX users are traditionally placed.
sys	3	This group has no specific meaning.
tty	4	A group that owns special files, such as the device file associated with an SSH or telnet user.
unknown	99	The group used when the system doesn't know about the hard drive.
utmp	45	The group that controls what can update the system's list of logged-in users.
uucp	66	The group used to control access to UUCP spool files.

Predefined group name	Group ID	Use
wheel	0	Another group (in addition to the admin group) to which users with administrator privileges belong.
www	70	The nonprivileged group that Apache uses for its processes that handle requests.

Setup Overview

These are the major user and group administration activities:

- Step 1: Before you begin, do some planning.
- Step 2: Set up directory domains in which user and group accounts will reside.
- Step 3: Configure server search policies so servers can find user and group accounts.
- Step 4: Set up share points for home directories.
- Step 5: Set up share points for group directories.
- Step 6: Create users.
- Step 7: Create groups.
- Step 8: Set up client computers.
- Step 9: Review user and group account information as needed.
- Step 10: Update users and groups as needed.
- Step 11: Perform ongoing user and group account maintenance.

Following is a summary of each of these activities. See the pages indicated for detailed information.

Step 1: Before you begin, do some planning

See “Before You Begin” on page 135 for a list of items to think about before you start creating a large number of users and groups.

Step 2: Set up directory domains in which user and group accounts will reside

Make sure you have created any directory domain in which you’ve decided to store user and group accounts. See Chapter 2, “Directory Services,” for instructions on creating shared, or network-visible, domains.

Make sure that any user who will be using Workgroup Manager to add and change users and groups in directory domains has directory domain administration privileges in the domains for which the user is responsible. You can use Workgroup Manager to add and change user and group accounts that reside in NetInfo or LDAPv3 directory domains.

If you will be using LDAPv2, read-only LDAPv3, BSD configuration file, or other read-only directory domains, make sure the domains are configured to support Mac OS X Server access and that they provide the data you need for user and group accounts. It may be necessary to add, modify, or reorganize information in a directory to provide the information in the format needed:

- Chapter 2, “Directory Services,” describes how to configure Mac OS X Server to access remote servers on which these domains reside to retrieve information.
- Appendix A, “Open Directory Data Requirements,” describes the user and group account data formats that Mac OS X expects. When you configure your Mac OS X Server directory services to use directory domains that do not reside on Mac OS X Server, you may need to refer to this appendix to determine the data mapping requirements for particular kinds of directory domains.

Step 3: Configure server search policies so servers can find user and group accounts

Make sure that the search policy of any server which needs to access user and group information to provide services for particular users is configured to do so. Chapter 2, “Directory Services,” tells you how to set up search policies.

Step 4: Set up share points for home directories

Before you assign a home directory to a user, you need to define the share point in which the home directory will reside. You also need to configure the share point to automatically mount on the user’s computer when he or she logs in. See “Distributing Home Directories Across Multiple Servers” on page 156 through “Setting Up NFS Home Directory Share Points” on page 160 for information about setting up share points.

Step 5: Set up share points for group directories

A group directory is like a home directory for group users. It is a directory for storing documents, applications, and other items you want to share among group members. See “Working With Volume Settings for Groups” on page 170 for information about setting up group directories.

Step 6: Create users

You can use Workgroup Manager to create user accounts in directory domains that reside on Mac OS X Server and in non-Apple LDAPv3 directory domains that have been configured for write access. See these sections for instructions:

- “Creating User Accounts in Directory Domains on Mac OS X Server” on page 137 and “Creating Read-Write LDAPv3 User Accounts” on page 138
- “Shortcuts for Working With Users and Groups” on page 176
- “Using Presets” on page 176
- “Importing and Exporting User and Group Information” on page 178

For working with read-only user accounts, see “Working With Read-Only User Accounts” on page 139.

For details about all the settings for a user account, see “Working With Basic Settings for Users” on page 139 through “Working With Managed Users” on page 154.

For details about setting up managed users, see Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8.” When you use managed users, creating users in a network directory domain is optional. All users can be locally defined on client computers.

Step 7: Create groups

You can use Workgroup Manager to create group accounts in directory domains that reside on Mac OS X Server and in non-Apple LDAPv3 directory domains that have been configured for write access. See these sections for instructions:

- “Creating Group Accounts in a Directory Domain on Mac OS X Server” on page 165 and “Creating Read-Write LDAPv3 Group Accounts” on page 166
- “Shortcuts for Working With Users and Groups” on page 176
- “Using Presets” on page 176
- “Importing and Exporting User and Group Information” on page 178

For working with read-only group accounts, see “Working With Read-Only Group Accounts” on page 167.

For details about all the settings for a group account, see “Working With Member Settings for Groups” on page 167 through “Working With Group and Computer Preferences” on page 173.

Step 8: Set Up Client Computers

Make sure that the directory services of Mac OS X computers are set up so they can access user accounts at login. See “Supporting Client Computers” on page 202 for details about how to configure Mac OS X computers as well as other client computers so that users can be authenticated and access the services you want them to.

Step 9: Review user and group account information as needed

Workgroup Manager makes it easy for you to review and optionally update information for users and groups. See the sections starting with “Finding User and Group Accounts” on page 173 for details.

Step 10: Update users and groups as needed

As users come and go and the requirements for your servers change, keep user and group records up to date. Information in these sections will be useful:

- “Working With Basic Settings for Users” on page 139 through “Working With Print Settings for Users” on page 151 describe all the user account settings you may need to change.
- “Defining a Guest User” on page 154 through “Disabling a User Account” on page 155 describe common user account maintenance activities.
- “Working With Member Settings for Groups” on page 167 describes the group account settings you may need to change.
- “Adding Users to a Group” on page 168, “Removing Users From a Group” on page 168, and “Deleting a Group Account” on page 173 describe some group maintenance activities.

Step 11: Perform ongoing user and group account maintenance

Information in these sections will help you with your day-to-day account maintenance activities:

- “Monitoring a Password Server” on page 197
- “Solving Problems” on page 202
- “Backing Up and Restoring Files” on page 201

Before You Begin

Before setting up user and group accounts for the first time:

- Identify the directory domains in which you will store user and group account information.

If you have an Active Directory or LDAP server already set up, you might be able to take advantage of existing records. See Chapter 2, “Directory Services,” for details about the directory domain options available to you.

If you have an earlier version of an Apple server, you might be able to migrate existing records. See *Upgrading to Mac OS X Server* for available options.

Create new directory domains as required to store user records. See Chapter 2, “Directory Services,” for instructions.

Note: If all the domains have not been finalized when you are ready to start adding accounts, simply add them to any domain that already exists on your server. (You can use the local directory domain—it’s always available.) You can move users and groups to another directory domain later by using your server’s export and import capabilities, described in “Importing and Exporting User and Group Information” on page 178.

- Determine which password verification policy or policies you will use. See “Understanding Password Validation” on page 189 for information about the options.
- Determine which users you want to make managed users. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for planning guidelines.
- Devise a home directory strategy.

Determine which users need home directories and identify the computers on which you want user home directories to reside. For performance reasons, avoid using network home directories over network connections slower than 100 Mbps. A user’s network home directory does not need to be stored on the same server as the directory domain containing the user’s account. In fact, distributing directory domains and home directories among various servers can help you balance your network workload. “Distributing Home Directories Across Multiple Servers” on page 156 and “Setting Up Home Directories for Users Defined in Existing Directory Servers” on page 157 describe several such scenarios.

You may want to store home directories for users with last names from A to F on one computer, G to J on another, and so on. Or you may want to store home directories on a Mac OS X Server but store user and group accounts on an Active Directory or LDAP server. Pick a strategy before creating users. You can move home directories, but if you do, you may need to change a large number of user and share point (mount) records.

Determine the access protocol to use for the home directories. Most of the time you will use AFP, but if you support a large number of UNIX clients with your server, you may want to use NFS for them. “Choosing a Protocol for Home Directories” on page 160 provides some information on this topic.

Once you have decided how many and which computers you want to use for home directories, plan the domain name or IP address of each computer. Also determine the names and any share points on computers that will be used for home directories.

- Determine the groups and workgroups you will need.

Users with similar server requirements should be placed in the same group.

Workgroups are useful when you want to set up group preferences. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for guidelines on using workgroups.

Determine where you want to store group directories.

- Decide who you want to be able to administer users and groups and make sure they have administrator privileges. “Administration Privileges” on page 125 describes administrator privileges.

When you use Server Assistant to initially configure your server, you specify a password for the owner/administrator. The password you specify also becomes the root password for your server. Use Workgroup Manager 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 Workgroup Manager to change the root password.

- Decide how you want to configure client computers so that the users you want to support can effortlessly log in and work with your server. Chapter 2, “Directory Services,” provides some information about this topic.

Administering User Accounts

This section describes how to administer user accounts stored in various kinds of directory domains.

Where User Accounts Are Stored

User accounts, as well as group accounts and computer accounts, can be stored in any Open Directory domain accessible from the Mac OS X computer that needs to access the account. A directory domain can reside on a Mac OS X computer (for example, a NetInfo or LDAPv3 domain) or it can reside on a non-Apple server (for example, an LDAP or Active Directory server).

You can use Workgroup Manager to work with accounts in all kinds of directory domains, but you can update only NetInfo and LDAPv3 directory domains using Workgroup Manager.

See Chapter 2, “Directory Services,” for complete information about the different kinds of Open Directory domains.

Creating User Accounts in Directory Domains on Mac OS X Server

You need administrator privileges for a directory domain to create a new user account in it.

To create a user account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the domain of interest. See Chapter 2, “Directory Services,” for instructions.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the domain in which you want the user’s account to reside.

- 4 Click the lock to be authenticated as a directory domain administrator.
- 5 From the Server menu, choose New User.
- 6 Specify settings for the user in the tabs provided. See “Working With Basic Settings for Users” on page 139 through “Working With Print Settings for Users” on page 151 for details.

You can also use a preset or an import file to create a new user. See “Using Presets” on page 176 and “Importing and Exporting User and Group Information” on page 178 for details.

Creating Read-Write LDAPv3 User Accounts

You can create a user account on a non-Apple LDAPv3 server if it has been configured for write access.

To create an LDAPv3 user account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to use the LDAP server for user accounts. See Chapter 2, “Directory Services,” for details about how to use Directory Access to configure an LDAP connection and Appendix A, “Open Directory Data Requirements,” for information about the user account elements that may need to be mapped.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the LDAPv3 domain in which you want the user’s account to reside.
- 4 Click the lock to be authenticated.
- 5 From the Server menu, choose New User.
- 6 Specify settings for the user in the tabs provided. See “Working With Basic Settings for Users” on page 139 through “Working With Print Settings for Users” on page 151 for details.

You can also use a preset or an import file to create a new user. See “Using Presets” on page 176 and “Importing and Exporting User and Group Information” on page 178 for details.

Changing User Accounts

You can use Workgroup Manager to change a user account that resides in a Mac OS X or non-Apple LDAPv3 directory domain.

To make changes to a user account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the directory domain of interest. See Chapter 2, “Directory Services,” for instructions.
- 2 In Workgroup Manager, click the Accounts button.

- 3 Use the At pop-up menu to open the domain in which the user's account resides.
- 4 Click the lock to be authenticated.
- 5 Click the User tab to select the user you want to work with.
- 6 Edit settings for the user in the tabs provided. See “Working With Basic Settings for Users” on page 139 through “Working With Print Settings for Users” on page 151 for details.

Working With Read-Only User Accounts

You can use Workgroup Manager to review information for user accounts stored in read-only directory domains. Read-only directory domains include LDAPv2 domains, LDAPv3 domains not configured for write access, and BSD configuration files.

To work with a read-only user account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the directory domain in which the account resides. See Chapter 2, “Directory Services,” for information about using Directory Access to configure server connections and Appendix A, “Open Directory Data Requirements,” for information about the user account elements that need to be mapped.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the directory domain in which the user's account resides.
- 4 Use the tabs provided to review the user's account settings. See “Working With Basic Settings for Users” on page 139 through “Working With Print Settings for Users” on page 151 for details.

Working With Basic Settings for Users

Basic settings are a collection of attributes that must be defined for all users.

In Workgroup Manager, use the Basic tab in the user account window to work with basic settings.

Defining User Names

The user name is the long name for a user. Sometimes the user name is referred to as the “real” name. Users can log in using the user name or a short name associated with their accounts.

A user name can contain as many as 255 characters (127 double-byte characters). Use only these characters:

- a through z
- A through Z

- 0 through 9
- _ (underscore)
- - (hyphen)
- . (period)
- (space)

For example, Dr. Arnold T. Smith.

You can use Workgroup Manager to edit the user name of an account stored in a directory domain residing on Mac OS X Server or in a non-Apple LDAPv3 directory domain or to review the user name in any directory domain accessible from the server you are using.

To work with the user name using Workgroup Manager:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user’s account resides. To change the name, click the lock to be authenticated. Select the user in the user list.
- 2 In the Name field on the Basic tab, review or edit the user name. Initially, the value of user name is “Untitled <some-number>.” After changing the name, Workgroup Manager does not check to verify that the user name is unique.

Defining Short Names

A *short name* is an abbreviated name for a user. Users can log in using the short name or the user name associated with their accounts. The short name is used by Mac OS X for home directories and groups:

- When Mac OS X automatically creates a user’s home directory, it names the directory after the user’s short name. See “Administering Home Directories” on page 155 for more information about home directories.
- When Mac OS X checks to see whether a user belongs to a group authorized to access a particular file, it uses short names to find UIDs of group members. See “Avoiding Duplicate Short Names” on page 143 for an example.

You can have as many as 16 short names associated with a user account, but the first one in the list must consist of all 7-bit ASCII characters, with no symbols or spaces. The first short name is the name used for home directories and group membership lists.

A short name can contain as many as 255 characters (127 double-byte characters). Use only these characters:

- a through z
- A through Z
- 0 through 9

- _ (underscore)
- - (hyphen)
- . (period)

Typically, short names contain eight or fewer characters.

You can use Workgroup Manager to edit the short name of an account stored in a directory domain on Mac OS X Server or a non-Apple LDAPv3 directory domain or to review the short name in any directory domain accessible from the server you are using.

To work with a user's short name using Workgroup Manager:

- 1** In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To change the short name, click the lock to be authenticated. Select the user in the user list.
- 2** In the Short Names field on the Basic tab, review or edit the short names. Initially, the value of the short name is "untitled_ <some-number>." If you specify multiple short names, each should be on its own line.

After the user's account has been saved, you cannot change the first short name, but you can change others in a list of short names.

Choosing Stable Short Names

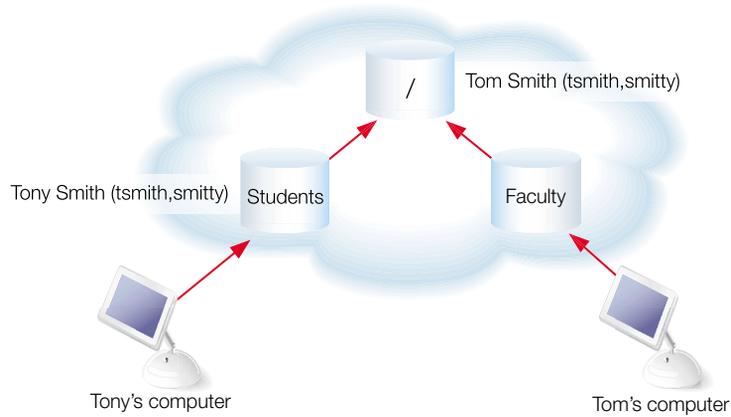
When you create groups, Mac OS X identifies users in them by their first short name, which can't be changed.

If a short name change is unavoidable, you can create a new account for the user (in the same directory domain) that contains the new short name, but retains all other information (UID, primary group, home directory, and so forth). Then disable login for the old user account. Now the user can log in using the changed name, yet have the same access to files and other network resources as before. (See "Disabling a User Account" on page 155 for information on disabling use of an account for login.)

Avoiding Duplicate Names

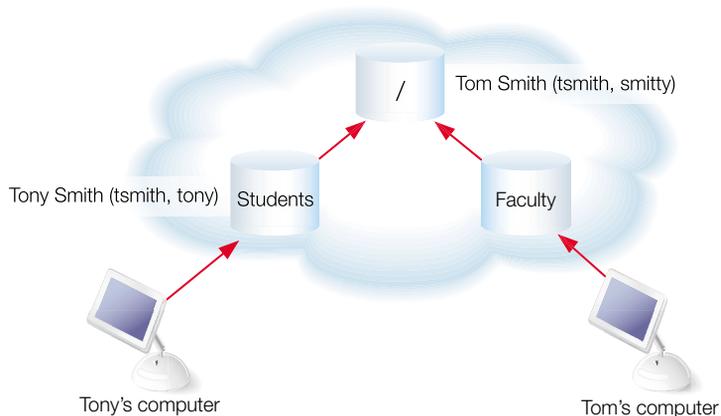
If separate user accounts have the same name (user name or short name) and password, a Mac OS X computer may authenticate a user different from the one you want it to authenticate. Or it may mask the user record that should be used for authentication.

Consider an example that consists of three shared directory domains. Tony Smith has an account in the Students domain, and Tom Smith has an account in the root domain. Both accounts contain the short name “tsmith” and the password “smitty.”



When Tony logs in to his computer with a user name “tsmith” and the password “smitty,” he is authenticated using the record in the Students domain. Similarly, Tom can use the same login entries at his computer and be authenticated using his record in the root domain. If Tony and Tom ever logged in to each other’s computers using tsmith and smitty, they would both be authenticated, but not with the desired results. Tony could access Tom’s files, and vice versa.

Now let’s say that Tony and Tom have the same short name, but different passwords.



If Tom attempts to log in to Tony’s computer using the short name “tsmith” and his password (smitty), his user record is masked by Tony’s user record in the Students domain. Mac OS X finds “tsmith” in Students, but its password does not match the one Tom used to log in. Tom is denied access to Tony’s computer, and his record in the root domain is never found.

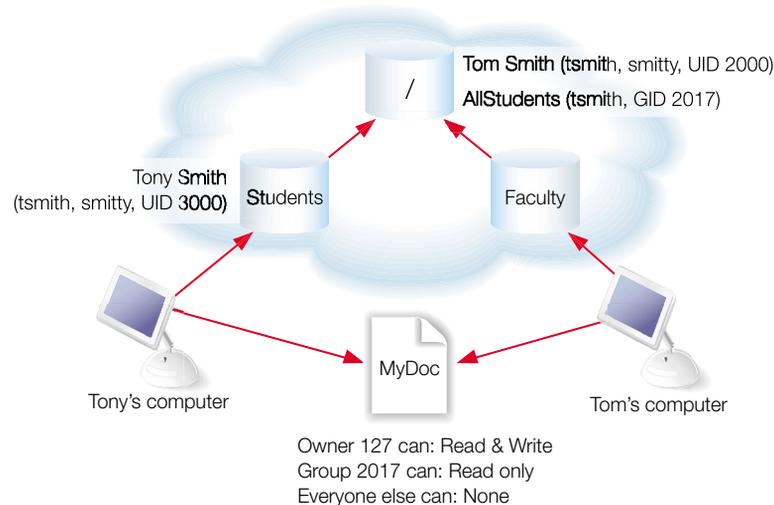
If Tony has a user record in his local directory domain that has the same names and password as his record in the Students domain, the Students domain's record for Tony would be masked. Tony's local domain should offer a name/password combination that distinguishes it from the Students domain's record. If the Students domain is not accessible (when Tony works at home, for example), he can log in using the local name and continue using his computer. Tony can still access local files created when he logged in using the Students domain if the UID in both records is the same.

Duplicate short names also have undesirable effects in group records, described in the next section.

Avoiding Duplicate Short Names

Since short names are used to find UIDs of group members, duplicate short names can result in file access being granted to users you hadn't intended to give access.

Return to the example of Tony and Tom Smith, who have duplicate short names. Assume that the administrator has created a group in the root domain to which all students belong. The group—AllStudents—has a GID of 2017.



Now suppose that a file, MyDoc, resides on a computer accessible to both Tony and Tom. The file is owned by a user with the UID 127. It has read-only access privileges for AllStudents. Tom is not a member of AllStudents, but the short name in his user record, “tsmith,” is the same as Tony’s, who *is* in AllStudents.

When Tom attempts to access MyDoc, Mac OS X searches the login hierarchy for user records with short names that match those associated with AllStudents. Tom's user record is found because it resides in the login hierarchy, and the UID in the record is compared with Tom's login UID. They match, so Tom is allowed to read MyDoc, even though he's not actually a member of AllStudents.

Defining User IDs

A *user ID (UID)* is a number that uniquely identifies a user. Mac OS X computers use the UID to keep track of a user's directory and file ownership. When a user creates a directory or file, the UID is stored as the creator ID. A user with that UID has read and write privileges to the directory or file by default.

The UID should be a unique string of digits from 500 through 2,147,483,647. Assigning the same UID to different users is risky, since two users with the same UID have identical directory and file access privileges.

The UID 0 is reserved for the root user. UIDs below 100 are reserved for system use; users with these UIDs can't be deleted and shouldn't be modified except to change the password of the root user.

You can use Workgroup Manager to edit the UID of an account stored in a NetInfo or LDAPv3 directory domain or to review the UID in any directory domain accessible from the server you are using.

To work with the UID using Workgroup Manager:

- 1** In Workgroup Manager, open the account you want to work with if it is not already open. To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To change the UID, click the lock to be authenticated. Select the user in the user list.
- 2** If you specify a value in the User ID field on the Basic tab, make sure it will be unique in the search policy of computers the user will log in to. When creating new user accounts in any shared directory domain, UIDs are automatically assigned; the value assigned is an unused UID (1025 or greater) in the server's search path. (New users created using the Accounts Preferences pane on Mac OS X Desktop computers are assigned UIDs starting at 501.)

Once UIDs have been assigned and users start creating files and directories throughout a network, you shouldn't change UIDs. One possible scenario in which you may need to change a UID is when merging users created on different servers into one new server or cluster of servers. The same UID may have been associated with a different user on the previous server.

Defining Passwords

See “Understanding Password Validation” on page 189 for details about setting up and managing passwords.

Assigning Administrator Rights for a Server

A user who has server administration privileges can control most of the server’s configuration settings and use applications, such as Server Status, that require a user to be a member of the server’s admin group.

You can use Workgroup Manager to assign server administrator privileges to an account stored in a NetInfo or LDAPv3 directory domain or to review the server administrator privileges in any directory domain accessible from the server you are using.

To work with server administrator privileges in Workgroup Manager:

- 1 To edit server administrator privileges, log in to Workgroup Manager by specifying the name or IP address of the server for which you want to grant administrator privileges.
- 2 Click the Account button.
- 3 Use the At pop-up menu to open the directory domain in which the user’s account resides.
- 4 To change the privileges, click the lock to be authenticated.
- 5 In the Basic tab, select the “User can administer the server” option to grant server administrator privileges.

Assigning Administrator Rights for a Directory Domain

A user who has administration privileges for an Apple directory domain is able to make changes to user, group, and computer accounts stored in that domain using Workgroup Manager. The changes the user can make are limited to those you specify.

You can use Workgroup Manager to assign directory domain administrator privileges for an account stored in a NetInfo or LDAPv3 directory domain or to review these privileges in any directory domain accessible from the server you are using.

To work with directory domain administrator privileges in Workgroup Manager:

- 1 To assign directory domain privileges, ensure the user has an account in the directory domain.
- 2 In Workgroup Manager, click the Account button.
- 3 Use the At pop-up menu to open the directory domain in which the user’s account resides.
- 4 To edit privileges, click the lock to be authenticated.
- 5 In the Basic tab, select the “User can administer this directory domain” option to grant privileges.

- 6 Click Privileges to specify what the user should be able to administer in the domain. By default, the user has no directory domain privileges.
- 7 To work with privileges to change user, group, or computer accounts, click the Users, Groups, or Computers tab, respectively.
- 8 Select a checkbox to indicate whether you want the user to be able to change account and/or preference settings. If a box is not checked, the user can view the account or preference information in Workgroup Manager, but not change it.
- 9 Select “For all ...” to allow the user to change information for all users, groups, or computers in the directory domain.

Select “For ... listed below” to limit the items a user can change to the list on the right. To add an item to the list, double-click the item in the “Available” list. To remove an item from the list, double-click it.

- 10 To give the user the ability to add and delete users, groups, or computer accounts, check the “Edit ... accounts” box and select “For all ...” .

Working With Advanced Settings for Users

Advanced settings include login settings, password validation policy, and a comment.

In Workgroup Manager, use the Advanced tab in the user account window to work with advanced settings.

Defining Login Settings

By specifying user login settings, you can

- Control whether the user can be authenticated using the account.
- Allow a managed user to simultaneously log in to more than one managed computer at a time or prevent the user from doing so.
- Indicate whether a user of a managed computer can or must select a workgroup during login or whether you want to avoid showing workgroups when the user logs in.
- Identify the default shell the user will use for command-line interactions with Mac OS X, such as `/bin/csh` or `/bin/tcsh`. The default shell is used by the Terminal application on the computer the user is logged in to, but Terminal has a preference that lets you override the default shell. The default shell is used by SSH (Secure Shell) or Telnet when the user logs in to a remote Mac OS X computer.

You can use Workgroup Manager to define login settings of an account stored in a NetInfo or LDAPv3 directory domain or to review login settings in any directory domain accessible from the server you are using.

To work with login settings using Workgroup Manager:

- 1** In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To edit settings, click the lock to be authenticated. Select the user in the user list.
- 2** Click the Advanced tab.
- 3** Select "Allow simultaneous login" to let a user log in to more than one managed computer at a time.
- 4** During Login pop-up menu options let you choose a workgroup option if the user is using a managed computer. Choose an option if appropriate.
- 5** Choose a shell from the Login Shell pop-up menu to specify the default shell for the user when logging in to a Mac OS X computer. Click Custom if you want to enter a shell that does not appear on the list. To make sure a user cannot access the server remotely using a command line, use the option None.

Defining a Password Validation Strategy

For details about setting up and managing passwords, see "Understanding Password Validation" on page 189.

Editing Comments

You can save a comment in a user's account to provide whatever documentation might help with administering the user. A comment can be as long as 32,676 characters.

You can use Workgroup Manager to define the comment of an account stored in a NetInfo or LDAPv3 directory domain or to review the comment in any directory domain accessible from the server you are using.

To work with a comment using Workgroup Manager:

- 1** In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To edit a comment, click the lock to be authenticated. Select the user in the user list.
- 2** Click the Advanced tab.
- 3** Edit or review the contents of the Comment field.

Working With Group Settings for Users

Group settings identify the groups a user is a member of.

In Workgroup Manager, use the Groups tab in the user account window to work with group settings.

See “Administering Group Accounts” on page 165 for information on administering groups.

Defining a User’s Primary Group

A primary group is the group to which a user belongs by default.

The ID of the primary group is used by the file system when the user accesses a file he or she does not own. The file system checks the file’s group privileges, and if the primary group ID of the user matches the ID of the group associated with the file, the user inherits group access privileges. The primary group offers the fastest way to determine whether a user has group privileges for a file.

The primary group ID should be a unique string of digits. By default, it is 20 (which identifies the group named “staff”), but you can change it. The maximum value is 2,147,483,647.

You can use Workgroup Manager to define the primary group ID of an account stored in a NetInfo or LDAPv3 directory domain or to review the primary group information in any directory domain accessible from the server you are using.

To work with a primary group ID using Workgroup Manager:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user’s account resides. To edit the primary group, click the lock to be authenticated. Select the user in the user list.
- 2 Click the Groups tab.
- 3 Edit or review the contents of the Primary Group ID field. The value must be associated with a group that already exists and that is accessible in the search path of computers using the user account. Workgroup Manager displays the full and short names of the group after you enter a primary group ID.

Adding a User to Groups

Add a user to a group when you want multiple users to have the same file access privileges or when you want to manage their Mac OS X preferences using workgroups or computer lists.

You can use Workgroup Manager to add a user to a group if the user and group accounts are in a NetInfo or LDAPv3 directory domain.

To add a user to a group using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Groups tab.
- 3 Click Add to open a drawer listing the groups defined in the directory domain you are working with. (To include system groups in the list, choose Preferences on the Workgroup Manager menu, then select “Show system users and groups.”)
- 4 Select the group, then drag it into the Other Groups list on the Groups tab.

Removing a User From a Group

You can use Workgroup Manager to remove a user from a group if the user and group accounts reside in a NetInfo or LDAPv3 directory domain.

To remove a user from a group using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Groups tab.
- 3 Select the group or groups from which you want to remove the user, then click Remove.

Reviewing a User's Group Memberships

You can use Workgroup Manager to review the groups a user belongs to if the user account resides in a directory domain accessible from the server you are using.

To review group memberships using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Select the user in the user list.

- 2 Click the Groups tab. The primary group to which the user belongs is displayed, and other groups the user belongs to are listed in the Other Groups list.

Working With Home Settings for Users

Home settings describe a user's home directory attributes. See “Administering Home Directories” on page 155 for information about using and setting up home directories.

Working With Mail Settings for Users

You can create a Mac OS X Server mail service account for a user by specifying mail settings for the user in the user's account. To use the account, the user simply configures a mail client to identify the user name, password, mail service, and mail protocol you specify in the mail settings.

In Workgroup Manager, use the Mail tab in the user account window to work with a user's mail service settings.

See Chapter 9, "Mail Service," for information about how to set up and manage Mac OS X Server mail service.

Disabling a User's Mail Service

You can use Workgroup Manager to disable mail service for a user whose account is stored in a NetInfo or LDAPv3 directory domain.

To disable a user's mail service using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Mail tab.
- 3 Select None.

Enabling Mail Service Account Options

You can use Workgroup Manager to enable mail service and set mail options for a user account stored in a NetInfo or LDAPv3 directory domain or to review the mail settings of accounts stored in any directory domain accessible from the server you are using.

To work with a user's mail account options using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Mail tab.
- 3 Selecting the Enabled button enables the user to use mail service.

- 4 The Mail Server field contains the DNS name or IP address of the server to which the user's mail should be routed. When you enter a value, Workgroup Manager does not check to ensure it is valid.
- 5 The Mail Quota field specifies the maximum number of megabytes for the user's mailbox. A 0 or null value means no quota is used. When the user's message space approaches or surpasses the mail quota you specify, mail service displays a message prompting the user to delete unwanted messages to free up space.
- 6 The Mail Access selection identifies the protocol used for the user's mail account: Post Office Protocol (POP) and/or Internet Message Access Protocol (IMAP).
- 7 The Options setting determines inbox characteristics for mail accounts that access email using both POP and IMAP.

"Use separate inboxes for POP and IMAP" creates an inbox for POP mail and a separate inbox for IMAP mail. "Show POP Mailbox in IMAP folder list" shows an IMAP folder named POP Inbox.
- 8 "Enable NotifyMail" lets you automatically notify the user's mail application when new mail arrives. The IP address to which the notification is sent can be either the last IP address from which the user logged in or an address you specify.

Forwarding a User's Mail

You can use Workgroup Manager to set up email forwarding for a user whose account is stored in a NetInfo or LDAPv3 directory domain.

To forward a user's mail using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
- 2 Click the Mail tab.
- 3 Select Forward and enter the forwarding email address in the Forward To field. The existence of the address is not verified by Workgroup Manager.

Working With Print Settings for Users

Print settings associated with a user's account define the ability of a user to print to accessible Mac OS X Server print queues for which print service enforces print quotas. "Enforcing Quotas for a Print Queue" on page 322 tells you how to set up quota-enforcing print queues.

In Workgroup Manager, use the Print tab in the user account window to work with a user's print quotas:

- Select None (the default) to disable a user's access to print queues enforcing print quotas.
- Select All Queues to let a user print to all accessible print queues that enforce quotas.
- Select Per Queue to let a user print to specific print queues that support quotas.

Disabling a User's Access to Print Queues Enforcing Quotas

You can use Workgroup Manager to prevent a user from printing to any accessible Mac OS X print queue that enforces quotas. To use Workgroup Manager, the user's account must be stored in a NetInfo or LDAPv3 directory domain.

To disable a user's access to print queues enforcing quotas:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Print tab.
- 3 Select None.

Enabling a User's Access to Print Queues Enforcing Quotas

You can use Workgroup Manager to allow a user to print to all or only some accessible Mac OS X print queues that enforce quotas. To use Workgroup Manager, the user's account must be stored in a NetInfo or LDAPv3 directory domain.

To set a user's print quota for print queues enforcing quotas:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

- 2 Click the Print tab.

To set up a quota that applies to all queues, go to step 3. Alternatively, to set up quotas for specific print queues, go to step 4.

- 3 Click "All Queues," then specify the maximum number of pages the user should be able to print in a certain number of days for any print queue enforcing quotas.

- 4 Click “Per Queue,” then use the Queue Name pop-up menu to select the print queue for which you want to define a user quota. If the print queue you want to specify is not on the Queue Name pop-up menu, click Add to enter the queue name and specify, in the Print Server field, the IP address or DNS name of the server where the queue is defined.

To give the user unlimited printing rights to the queue, click “Unlimited printing.” Otherwise, specify the maximum number of pages the user should be able to print in a certain number of days. Then click Save.

Deleting a User’s Print Quota for a Specific Queue

To delete a user’s print quota using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
- 2 Click the Print tab.
- 3 Use the Queue Name pop-up menu and the Print Server field to identify the print queue to which you want to disable a user’s access.
- 4 Click Delete.

Restarting a User’s Print Quota

To restart a user’s print quota using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to work with if it is not already open.

To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
- 2 Click the Print tab.
- 3 If the user is set up for printing to all print queues supporting quotas, click Restart Print Quota.

If the user’s print quotas are print queue–specific, use the Queue Name pop-up menu and the Print Server field to identify a print queue, then click Restart Print Quota.

Working With Managed Users

See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for information about how you can make a user a managed user, which lets you set up preferences for the user.

Defining a Guest User

You can set up some services to support users who are anonymous, that is, they can't be authenticated because they do not have a valid user name or password. The following services can be set up this way:

- Windows services (see “Windows Services” on page 235 for information about configuring guest access)
- Apple file service (see “Apple File Service” on page 224 for information about configuring guest access)
- FTP service (see “File Transfer Protocol (FTP) Service” on page 244 for information about configuring guest access)
- Web service (see Chapter 8, “Web Service,” for information about configuring guest access)

Users who connect to a server anonymously are restricted to files, folders, and Web sites with privileges set to Everyone.

Another kind of guest user is a managed user that you can define to allow easy setup of public computers or kiosk computers. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for more about these kinds of users.

Deleting a User Account

You can use Workgroup Manager to delete a user account stored in a NetInfo or LDAPv3 directory domain.

To delete a user account using Workgroup Manager:

- 1 In Workgroup Manager, open the user account you want to delete if it is not already open.
To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.
- 2 Choose Delete Selected User from the Server menu.

Disabling a User Account

To disable a user account, you can

- delete the account (see “Deleting a User Account” on page 154)
- change the user’s password to an unknown value (see “Defining Passwords” on page 145)

Administering Home Directories

A home directory is a folder for a user’s personal use. Mac OS X also uses the home directory, for example, for storing system preferences and managed user settings for Mac OS X users.

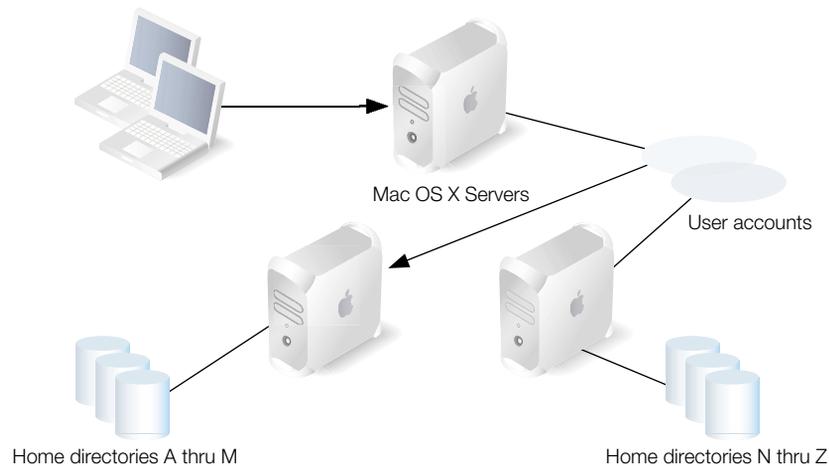
A user’s home directory does not need to be stored on the same server as the directory domain containing the user’s account. In fact, distributing directory domains and home directories among various servers can help you balance your workload among several servers. “Distributing Home Directories Across Multiple Servers” on page 156 and “Setting Up Home Directories for Users Defined in Existing Directory Servers” on page 157 describe several such scenarios.

After deciding where you want home directories to reside, you need to set up share points for them and configure the share points to automount. You may also need to create home directory folders. See “Setting Up AFP Home Directory Share Points” on page 160 and “Creating Home Directory Folders” on page 161 for details.

To assign a home directory to a user, follow the instructions in “Defining a User’s Home Directory” on page 161 through “Using Import Files to Create AFP Home Directories” on page 165.

Distributing Home Directories Across Multiple Servers

The following illustration depicts using one Mac OS X Server for storing user accounts and two other Mac OS X Servers for storing AFP home directories.



When a user logs in, he or she is authenticated using an account stored on the accounts server. The location of the user's home directory, stored in his account, is used to mount his or her home directory, which resides physically on one of the home directory servers.

Here are the steps you could use to set up this scenario for AFP home directories:

- 1 Set up the directory services of the client computers so their search policy includes the server where the user accounts are stored. See Chapter 2, "Directory Services," for instructions.
- 2 On each home directory server, create the folder that will serve as the share point for the home directories. Set up automounting for each share point. Doing so ensures that a user can automatically see his home directory after logging in because it is mounted on his computer. See "Setting Up AFP Home Directory Share Points" on page 160 for more information about setting up AFP share points for home directories.

When you set up automounting, Mac OS X Server creates a mount record for the share point in the directory domain you designate. The mount record that describes home directory share points can reside in the same directory domain as the user account or in a directory domain in the search path used to find related user records.

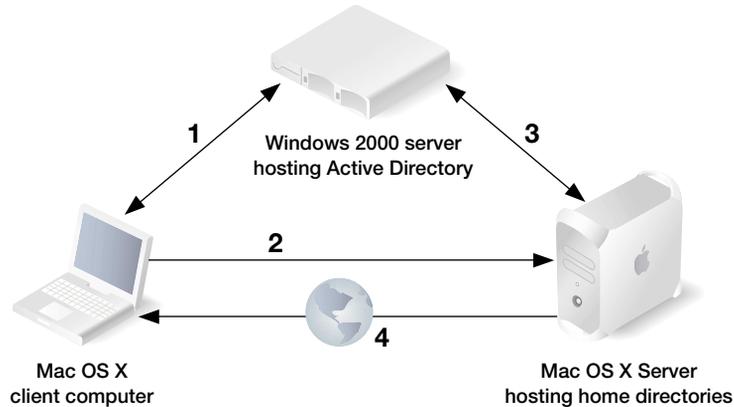
- 3 Set up the user accounts on the account server so that the home directory share point is one of the two you created in step 1. See "Defining a Network Home Directory" on page 163.

Because the home directories are accessed using AFP, the first time a user logs in his or her home directory is created automatically on the appropriate server and is visible on the user's computer.

Setting Up Home Directories for Users Defined in Existing Directory Servers

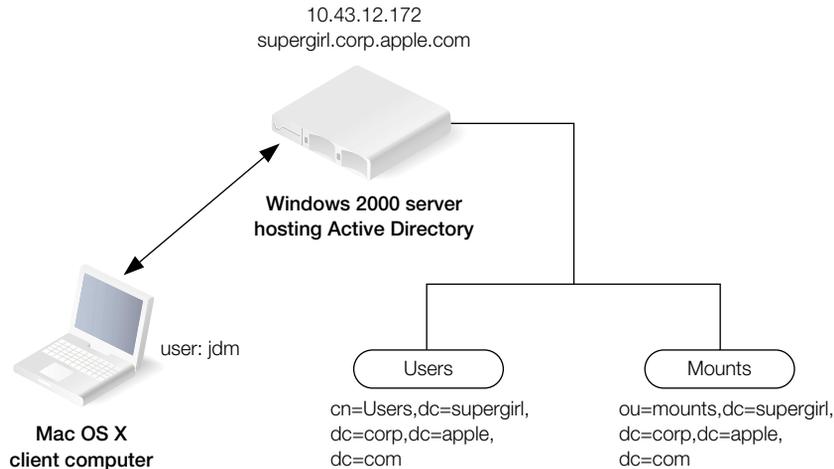
When you integrate Mac OS X Server into an environment that uses an existing directory server for storing user information, you can take advantage of that information for authenticating users, but use one or more Mac OS X Servers to store home directories for users.

The following picture illustrates this scenario. A user has access to his home directory on Mac OS X Server after logging in to a Mac OS X computer and being authenticated using Active Directory information.



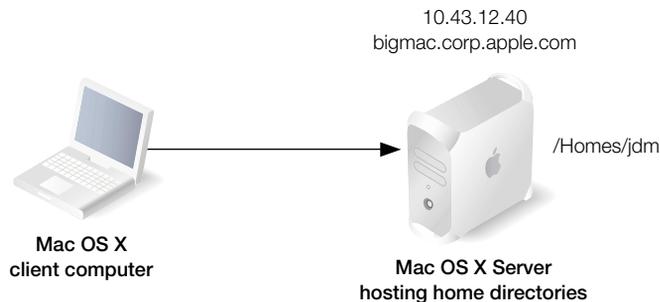
The numbers in this figure illustrate the sequence of interactions that occur between the time a user logs in to the Mac OS X client computer and can choose Home from the Go menu to access his home directory:

- 1 Retrieving user information. When the user logs in, the Mac OS X computer retrieves the user's account from Active Directory and authenticates the user. Home directory information in the user's record indicates that the home directory resides on the network, so a mount record for the home directory is retrieved from Active Directory. The mount record identifies the home directory share point and its access protocol—AFP in this case.



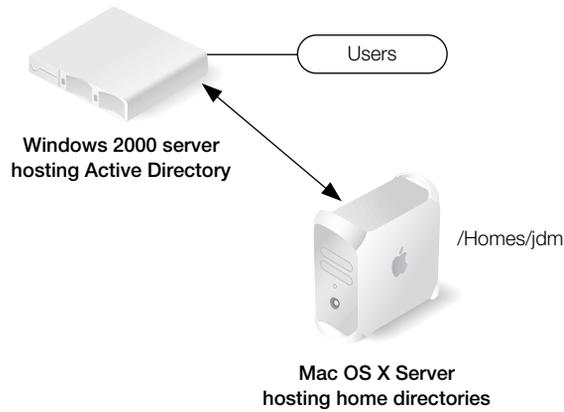
In this example, the user and mount records reside in the search bases indicated in Active Directory on the Windows 2000 Server. A search base is like a directory you use to access particular kinds of records.

- 2 Requesting authorization to mount the home directory. The Mac OS X client computer then sends the user's information to the Mac OS X Server hosting the home directory to request authorization to mount the home directory.

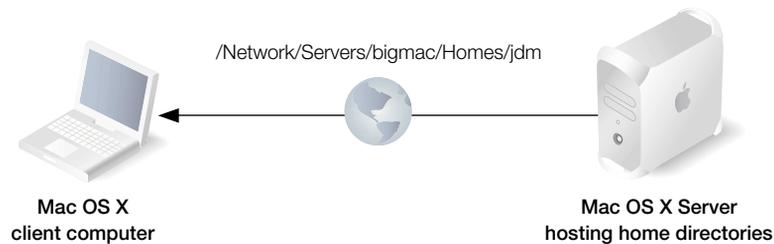


The home directories, named using the user short names, reside under the share point named “Homes” on Mac OS X Server.

- 3 Setting up home directory access. Next, the server retrieves the user's Active Directory record and authenticates the user. The server uses the UID and group ID in the record to set up file access permissions for the user.



- 4 Accessing the home directory. The home directory is now mounted and visible on the user's computer in the Mac OS X Finder under /Network/Servers/bigmac/Homes, and login is complete.



Here are the steps you would use to set up this scenario:

- 1 Set up the Windows server to make sure Active Directory contains the necessary user account and mount data.
- 2 Set up directory service mappings for Mac OS X computers, both clients and server, so they can access the Active Directory data. See Chapter 2, "Directory Services," information about using the Active Directory mapping template and add the Windows server to the Mac OS X computer's search policies.
- 3 Set up share points on Mac OS X Server.

Because the home directories are accessed using AFP, the first time a user logs in his home directory is created automatically and is visible on the user's computer.

Choosing a Protocol for Home Directories

You can set up home directories so they can be accessed using either AFP or NFS.

The preferred protocol is AFP, because it provides authentication-level access security; a user has to log in with a valid name and password to access files. AFP also simplifies the setup of home directories; home directories are automatically created the first time a user logs in.

Use NFS only if you need to provide home directories for a large number of users who use UNIX workstations. NFS file access is based not on user authentication, but on client IP address, so it is generally less secure than AFP. In addition, NFS home directories need to be created manually.

See the next two sections information about using AFP and NFS protocols for home directories.

Setting Up AFP Home Directory Share Points

Before setting up an AFP home directory for a user, define an automountable share point in which the home directory will reside. Setting up a home directory in an automountable share point makes the home directory available in `/Network/Servers` and lets other users access the home directory using the `~username` shortcut.

Because of the way home directory disk quotas work, you may want to set up home directory share points on a partition different from other share points. See “Setting Disk Quotas” on page 164 for more information.

To define an AFP share point for home directories:

- 1 Create a folder on the server where you want the home directories to reside, and share the folder using AFP. See Chapter 4, “Sharing,” for complete instructions on how to accomplish this and the remaining steps.
- 2 Enable guest access to the share point so users can access other users’ public folders without authenticating. Also, ensure that the share point owner has Read & Write privileges and that Group and Everyone have Read privileges.
- 3 Configure a mount record for the share point. To do so, set up the share point to automount, using AFP, in a directory domain in the search path of Mac OS X computers that need to use it.

Setting Up NFS Home Directory Share Points

Before setting up an NFS home directory for users, define the share point in which the home directories will reside. Because NFS offers less access security than AFP, define one NFS share point for use by all UNIX users who need home directories.

Because of the way home directory disk quotas work, you may want to set up home directory share points on a partition different from other share points. See “Setting Disk Quotas” on page 164 for more information.

To define an NFS share point for home directories:

- 1** Create a folder on the server where you want the home directories to reside, and share the folder using NFS. See Chapter 4, “Sharing,” for complete instructions on setting up NFS share points.
- 2** Export the share point, use the pop-up menu to select the clients to whom you want to export the share point, and map the “root” user to “nobody.”
- 3** Configure a mount record for the share point. To do so, set up the share point so it is automounted, using NFS, in a directory domain in the search path of Mac OS X computers that need to use it.
- 4** In the share point folder, manually create the home directory folder and all its subfolders for each user.

UNIX users are accustomed to using SSH to obtain command-line access to a server. With this kind of access, the user’s home directory isn’t mounted, and the user has only guest access to it.

Creating Home Directory Folders

AFP home directories and their subfolders are created automatically when users first log in.

NFS home directories must be created manually within the folder that serves as the NFS share point.

Defining a User’s Home Directory

In Workgroup Manager, use the Home tab in the user account window to work with home directory settings for a user.

- Select Local to define a home directory on the server you are using for a user defined in a local directory domain on that server.
- Select Network to set up a home directory for users defined in shared directory domains. The home directory resides immediately under a share point you select from a list of automountable share points in directory domains of the server’s search path.
- Select the Advanced option to set up a home directory that has characteristics not available using the Local or Network options. For example, the Advanced option lets you set up a network home directory that is not immediately below the share point.

The next four sections describe how to use the user account Home tab.

You can also use an import file to set up home directories. See “Using Import Files to Create AFP Home Directories” on page 165 for details.

Defining No Home Directory

You can use Workgroup Manager to avoid creating a home directory for a user whose account is stored in a NetInfo or LDAPv3 directory domain. By default, new users have no home directory.

To define no home directory:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the local directory domain. To edit the home directory information, click the lock to be authenticated, then select the user in the user list.
- 2 Click the Home tab.
- 3 Select No Home.

Defining a Home Directory for Local Users

You can use Workgroup Manager to define a home directory for a user whose account is stored in the local directory domain on the server you are logged in to. Local user accounts are visible only on the server itself, not over the network. Local user accounts on Mac OS X Server are most useful for standalone servers (servers not accessible from a network) and server administrator accounts.

To create a home directory for a local user account:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the local directory domain. To edit the home directory information, click the lock to be authenticated, then select the user in the user list.
- 2 Click the Home tab.
- 3 Select Local, then choose the share point from the Share Point pop-up menu in which you want the home directory to reside. By default, /Users is assumed, but you can select any other share point that has been defined in the local directory domain. The share point does not have to be configured for automounting.

If the home directory share point is an AFP share point, the home directory is created automatically when the user logs in if it does not already exist; the name of the home directory created is the same as the user's short name (the user's first short name if there are multiple short names). If it is an NFS share point, you must create the home directory and its subfolders manually.

Defining a Network Home Directory

In Workgroup Manager, you can set up a home directory for users defined in shared directory domains. The home directory resides immediately under an automountable share point.

You can use Workgroup Manager to define a network home directory for a user whose account is stored in a NetInfo or LDAPv3 directory domain or to review home directory information in any directory domain accessible from the server you are using.

To create a network home directory using Workgroup Manager:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To edit the home directory information, click the lock to be authenticated, then select the user in the user list.
- 2 Click the Home tab, then select Network.
- 3 Select a share point from the list, which displays all the network-visible share points in the search path of the server you are using.

If the home directory share point you select is an AFP share point, the home directory is created automatically when the user logs in if it does not already exist; the home directory is named after the user's short name (the first short name if the user has multiple short names). If it is an NFS share point, you must create the home directory and its subfolders manually.

Defining an Advanced Home Directory

In Workgroup Manager, you can customize a user's home directory settings using the Advanced home directory option. You'll want to customize home directory settings when

- You want the user's home directory to reside in directories not immediately below the home directory share point. For example, you may want to organize home directories into several subdirectories within a share point. If Homes is the home directory share point, you may want to place teachers' home directories in Homes/Teachers and student home directories in Homes/Students.
- You want to specify a home directory name different from the user's short name.

You can use Workgroup Manager to define an advanced home directory for a user whose account is stored in a NetInfo or LDAPv3 directory domain or to review home directory information in any directory domain accessible from the server you are using.

To create an advanced home directory using Workgroup Manager:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To edit the home directory information, click the lock to be authenticated, then select the user in the user list.

2 Click the Home tab, then select Advanced.

3 In the Server/Share Point URL field, enter the full URL to an existing share point.

For example, enter "AFP://server.example.com/Homes". Make sure that the share point has been set up as an automount.

4 In the Path field, enter the path from the share point to the home directory if there is one. Any directories you enter must exist.

For example, if the share point is Homes, you might enter Teachers/SecondGrade

5 In the Home field, enter the full path to the home directory.

For example, /Network/Servers/server.example.com/Homes/Teachers/SecondGrade/Smith.

If the home directory share point you select is an AFP share point on Mac OS X Server, the home directory is created automatically when the user logs in if it does not already exist; the home directory is named after the user's short name (the first short name if the user has multiple short names). If it is an NFS share point, you must create the home directory and its subfolders manually.

Setting Disk Quotas

You can limit the disk space a user can consume to store files he or she owns in the partition where his home directory resides.

This quota does not apply to the home directory share point or to the home directory, but to the entire partition within which the home directory share point and the home directory reside. Therefore when a user places files into another user's folder, it can have implications on the user's disk quota:

- When you copy a file to a user's AFP drop box, the owner of the drop box becomes the owner of the file.
- In NFS, however, when you copy a file to another folder, you remain the owner and the copy operation decrements *your* disk quota on a particular partition.

To set up a home directory share point disk quota using Workgroup Manager:

1 In Workgroup Manager, open the account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. To edit the disk quota, click the lock to be authenticated, then select the user in the user list.

2 Click the Home tab.

- 3 Specify the disk quota using the Disk Quota field and the adjacent pop-up menu.

Defining Default Home Directories for New Users

You can define default home directory settings to use for new users by using a preset to predefine them. See “Using Presets” on page 176 for information about defining and using presets.

Using Import Files to Create AFP Home Directories

The fastest way to create AFP home directories for a large number of users is to use an import file. See “Importing and Exporting User and Group Information” on page 178 for details.

Moving Home Directories

If you need to move a home directory, create the new one and manually delete the existing one to deallocate disk space it uses if you no longer need the existing one.

Deleting Home Directories

When you delete a user account, the associated home directory is not automatically deleted. You must delete it manually.

Administering Group Accounts

This section describes how to administer group accounts stored in various kinds of directory domains.

Where Group Accounts Are Stored

Group accounts, as well as user accounts and computer accounts, can be stored in any Open Directory domain accessible from the Mac OS X computer that needs to access the account. A directory domain can reside on a Mac OS X computer (for example, a NetInfo or LDAPv3 domain) or it can reside on a non-Apple server (for example, an LDAP or Active Directory server).

You can use Workgroup Manager to work with accounts in all kinds of directory domains, but you can only update NetInfo and LDAPv3 directory domains using Workgroup Manager.

See Chapter 2, “Directory Services,” for complete information about the different kinds of Open Directory domains.

Creating Group Accounts in a Directory Domain on Mac OS X Server

You need administrator privileges for a directory domain to create a new group account in it.

To create a group account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the domain of interest. See Chapter 2, “Directory Services,” for instructions.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the domain in which you want the group account to reside.
- 4 Click the lock to be authenticated as a directory domain administrator.
- 5 From the Server menu, choose New Group.
- 6 Specify settings for the group in the tabs provided. See “Working With Member Settings for Groups” on page 167 and “Working With Volume Settings for Groups” on page 170 for details.

You can also use a preset or an import file to create a new group. See “Using Presets” on page 176 and “Importing and Exporting User and Group Information” on page 178 for details.

Creating Read-Write LDAPv3 Group Accounts

You can create a group account on a non-Apple LDAPv3 server if it has been configured for write access.

To create an LDAPv3 group account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to use the LDAP server for group accounts. See Chapter 2, “Directory Services,” for information about using Directory Access to configure an LDAP connection and Appendix A, “Open Directory Data Requirements,” for information about the group account elements that may need to be mapped.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the LDAPv3 domain in which you want the group account to reside.
- 4 Click the lock to be authenticated.
- 5 From the Server menu, choose New Group.
- 6 Specify settings for the group in the tabs provided. See “Working With Member Settings for Groups” on page 167 and “Working With Volume Settings for Groups” on page 170 for details.

You can also use a preset or an import file to create a new group. See “Using Presets” on page 176 and “Importing and Exporting User and Group Information” on page 178 for details.

Changing Group Accounts

You can use Workgroup Manager to change a group account that resides in a NetInfo or LDAPv3 directory domain.

To make changes to a group account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the directory domain of interest. See Chapter 2, “Directory Services,” for instructions.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the domain in which the group account resides.
- 4 Click the lock to be authenticated.
- 5 Click the Group tab to select the group you want to work with.
- 6 Edit settings for the group in the tabs provided. See “Working With Member Settings for Groups” on page 167 and “Working With Volume Settings for Groups” on page 170 for details.

Working With Read-Only Group Accounts

You can use Workgroup Manager to review information for group accounts stored in read-only directory domains. Read-only directory domains include LDAPv2 domains, LDAPv3 domains not configured for write access, and BSD configuration files.

To work with a read-only group account:

- 1 Ensure that the directory services of the Mac OS X Server you are using has been configured to access the directory domain in which the account resides. See Chapter 2, “Directory Services,” for information about using Directory Access to configure server connections and Appendix A, “Open Directory Data Requirements,” for information about the group account elements that need to be mapped.
- 2 In Workgroup Manager, click the Accounts button.
- 3 Use the At pop-up menu to open the directory domain in which the group account resides.
- 4 Use the tabs provided to review the group account settings. See “Working With Member Settings for Groups” on page 167 and “Working With Volume Settings for Groups” on page 170 for details.

Working With Member Settings for Groups

Member settings include a group’s names, its ID, and a list of the users who are members of the group.

In Workgroup Manager, use the Members tab in the group account window to work with member settings.

When the name of a user in the Members list appears in *italics*, the group is the user's primary group.

Adding Users to a Group

Add users to a group when you want multiple users to have the same file access privileges or when you want to make them managed users.

When you create a user account and assign the new user a primary group, the user is automatically added to the group you specify; you do not need to explicitly do so. Otherwise, you explicitly add users to a group.

You can use Workgroup Manager to add users to a group if the user and group accounts are in a NetInfo or LDAPv3 directory domain.

To add users to a group using Workgroup Manager:

- 1 In Workgroup Manager, open the group account you want to work with if it is not already open. To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the group in the group list.
- 2 Click the Members tab.
- 3 Click Add to open a drawer listing the users defined in the directory domain you are working with. (To include system users in the list, choose Preferences on the Workgroup Manager menu, then select "Show system users and groups.") Make sure that the group account resides in a directory domain specified in the search policy of computers the user will log in to.
- 4 Select the user, then drag it into the Members list on the Members tab.

Removing Users From a Group

You can use Workgroup Manager to remove a user from a group that is not the user's primary group if the user and group accounts reside in a NetInfo or LDAPv3 directory domain.

To remove a user from a group using Workgroup Manager:

- 1 In Workgroup Manager, open the group account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the group in the group list.

- 2 Click the Members tab.
- 3 Select the user or users you want to remove from the group, then click Remove.

Naming a Group

A group has two names: a full name and a short name:

- The full group name, which is used for display purposes only, can contain as many as 255 characters (127 double-byte characters). Use only these characters:

a through z

A through Z

0 through 9

_ (underscore)

- (hyphen)

. (period)

(space)

For example, English Department Students.

- The short name can contain as many as 255 characters (127 double-byte characters). Use only these characters:

a through z

A through Z

0 through 9

_ (underscore)

- (hyphen)

. (period)

The short name, typically 8 or fewer characters, is used by Mac OS X to find UIDs of group members when determining whether a user can access a file as a result of his or her group membership.

You can use Workgroup Manager to edit the names of a group account stored in a NetInfo or LDAPv3 directory domain or to review the names in any directory domain accessible from the server you are using.

To work with group names using Workgroup Manager:

- 1 In Workgroup Manager, open the group account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. To change a name, click the lock to be authenticated. Select the group in the group list.

- 2 In the Name or “Short name” field on the Members tab, review or edit the names. Before saving a new name, Workgroup Manager checks to ensure that it is unique.

Defining a Group ID

A group ID is a string of ASCII digits that uniquely identifies a group. The maximum value is 2,147,483,647. The minimum value is 101.

You can use Workgroup Manager to edit the ID for a group account stored in a NetInfo or LDAPv3 directory domain or to review the group ID in any directory domain accessible from the server you are using.

To work with a group ID using Workgroup Manager:

- 1 In Workgroup Manager, open the group account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. To change a group ID, click the lock to be authenticated. Select the group in the group list.
- 2 In the Group ID field on the Members tab, review or edit the ID. Before saving a new group ID, Workgroup Manager checks to ensure that it is unique in the directory domain you are using.

Working With Volume Settings for Groups

You can designate a directory for use exclusively by members of a particular group. A group directory offers a way to organize documents and applications of special interest to group members and gives group members a directory to use to pass information back and forth among them.

If the group is a workgroup (if you want to define Mac OS X preferences for the group), you *must* set up a group volume. A workgroup’s preferences are stored in the group volume you associate with the workgroup.

In Workgroup Manager, use the Volumes tab in the group account window to work with group volume settings:

- Select None to avoid creating a group directory.
- Select Network to automate the creation of group volumes.
- Select Advanced to customize your group volume settings.

Before you can set up a group directory, you must create the share point for it to reside in, as the next section describes.

Creating Group Directories

Before you can designate a directory as a group directory, you must create a share point for the directory. Chapter 4, “Sharing,” tells you how to use Workgroup Manager to create a folder and share it.

If you are using AFP to share the group directory, you can take advantage of automatic group share point and group directory creation by choosing the Network option on the Volumes tab for the group account in Workgroup Manager. To work with other sharing protocols and share points, you must use the Advanced option on that tab.

Automatically Creating Group Directories

When you initially set up a server, an AFP share point named /groups is created automatically. You can automate the (overnight) creation of group directories in the /groups share point when you use Workgroup Manager to define groups in a NetInfo or LDAPv3 directory domain.

To set up an automatically created group directory:

- 1 In Workgroup Manager, open the group account you want to work with if it is not already open.

To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. To edit the group directory information, click the lock to be authenticated. Select the group in the group list.

- 2 Click the Volumes tab.
- 3 Select Network.
- 4 Click Select to choose a server from a list of servers that host a /groups share point in a directory domain in your current search path. The group directory is created immediately below it using the group’s short name. The server name you choose appears in the Server field.

Alternatively, enter a server name in the Server field. The group directory is created automatically only if the server you specify hosts a /groups share point in your current search path. Otherwise, you need to create an AFP share point on that server named /groups and, within it, a group directory with the short name of the group.

- 5 In the Owner Name field, enter the name of the user you want to own the group directory so he or she can act as group directory administrator. Click Users to choose an owner from a list of users in the current directory domain.
- 6 Optionally check one of the boxes that automate visibility of the group directory for group members when they log in to a Mac OS X computer.

Check “Show group documents” to automatically display the group directory in the Dock.

Check “Mount group volume at startup” to automatically display the group directory in the Finder.

Customizing Group Directory Settings

When you need more control over group directory settings than the network group directory option provides, you can use Workgroup Manager to customize group directory settings. The group whose directory you want to customize must be defined in a NetInfo or LDAPv3 directory domain.

For example, you may want to organize group directories as several folders within a share point. If LanguageGroups is a group directory share point, you may want to place the group directory for English students in LanguageGroups/English and for French students in LanguageGroups/French.

To customize group settings:

- 1 In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the group account resides. To edit the group directory information, click the lock to be authenticated, then select the group in the group list.
- 2 Click the Volumes tab, then select Advanced.
- 3 In the URL field, enter the full URL to the group directory’s share point.
For example, enter “SMB://ntserver.com/macgroups” to identify an SMB share point named “macgroups” on a server whose domain name is “ntserver.com”. The share point must already exist on the server.
- 4 In the Path field, enter the path from the share point to the group directory
For example, if the share point is GroupDirs and the full path to the group directory is GroupDirs/Teachers/Primary/, enter Teachers/Primary in the Path field. These directories must already exist.
- 5 In the Owner Name field, enter the name of the user you want to own the group directory so he or she can act as group directory administrator. Click Users to choose an owner from a list of users in the current directory domain.
- 6 Optionally check one of the boxes that automate visibility of the group directory for group members when they log in to a Mac OS X computer.
Check “Show group documents” to automatically display the group directory in the Dock.
Check “Mount group volume at startup” to automatically display the group directory in the Finder.

Working With Group and Computer Preferences

See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8,” for information about how you can use groups when you want managed Mac OS X users to have workgroup and computer list preferences.

Deleting a Group Account

You can use Workgroup Manager to delete a group account stored in a NetInfo or LDAPv3 directory domain.

To delete a group account using Workgroup Manager:

- 1 In Workgroup Manager, open the group account you want to delete if it is not already open. To open the account, click the Account button, then use the At pop-up menu to open the directory domain where the account resides. Click the lock to be authenticated. Select the group in the group list.
- 2 Choose Delete Selected Group from the Server menu.

Finding User and Group Accounts

In Workgroup Manager, user and group accounts are listed in tabs at the left side of the Workgroup Manager window.

Workgroup Manager preferences affect the lists. Choose the Preferences command on the Workgroup Manager menu to control whether system users and groups are listed and the order in which items are listed.

To work with one or more of the accounts listed, select them. Data about the selected accounts appears in tabs to the right of the list.

To populate the list, use the At menu to select the directory domain(s) you want to work with. Initially, the local directory domain accounts are listed. The domains available for selection include all directory domains configured for access by the server you are logged in to. “Listing Users and Groups in the Local Directory Domain” on page 174 through “Refreshing User and Group Lists” on page 175 tell you how to use the At menu.

Choose the Show Status Bar command on the View menu to display information related to your current At menu selection:

- When Search Path is selected, the status bar identifies the computer you are currently logged in to and the user name under which you are logged in.
- When “Other” or “Local” is selected, the status bar identifies the directory domain in which you are currently authenticated and the user name under which you are authenticated.

After you choose directory domains, all the accounts residing in those domains are listed. You can sort the list by clicking a column heading. You can filter the list to find specific users or groups by using the filter options above the list. See “Finding Specific Users and Groups in a List” on page 175 and “Sorting User and Group Lists” on page 175 for details.

Listing Users and Groups in the Local Directory Domain

The local directory domain is a server-resident domain that is visible only when you are logged in to the server where it resides.

To list accounts in the local domain of the server you are working with:

- 1 In Workgroup Manager, log in to the server hosting the domain, then select Local in the At pop-up menu.
- 2 User accounts residing in the local domain are listed in the user tab, and local group accounts are listed in the group tab. To work with a particular account, select it. To change the account, which requires that you have server or domain administrator privileges, click the lock to authenticate.

Listing Users and Groups in Search Path Directory Domains

The search path directory domains are those in the search policy defined for the Mac OS X Server you are logged in to.

To list accounts in search path domains of the server you are working with:

- 1 In Workgroup Manager, log in to a server whose search policy contains the directory domains of interest.
- 2 Select Search Path in the At pop-up menu.

User accounts residing in all directory domains in the search path are listed in the user tab, and group accounts are listed in the group tab.

- 3 To work with a particular account, select it. To change the account, which requires that you have server or domain administrator privileges, click the lock to authenticate.

Listing Users and Groups in Available Directory Domains

You can list user and group accounts residing in any specific directory domain accessible from the server you are logged in to using Workgroup Manager. You select the domain from a list of all the directory domains configured to be visible from the server you are using.

Note that “available” directory domains are not the same as directory domains in a search policy. A search policy consists of the directory domains a server searches routinely when it needs to retrieve, for example, a user’s account. But the same server might be configured to access directory domains that have not been added to its search policy.

To list accounts in directory domains accessible from a server:

- 1** In Workgroup Manager, log in to a server from which the directory domains of interest are visible.
- 2** Select Other in the At pop-up menu.
- 3** In the dialog box that appears, select the domain(s), then click OK.

User accounts residing in selected directory domains are listed in the user tab, and group accounts are listed in the group tab.

- 4** To work with a particular account, select it. To change a NetInfo or LDAPv3 account, which requires that you have server or domain administrator privileges, click the lock to authenticate.

Refreshing User and Group Lists

To refresh the list of user and group accounts currently displayed in Workgroup Manager, you can

- type in the field above the list
- choose another item in the At pop-up menu, then reselect the domain(s) you had been working with

User and group lists are automatically refreshed at the rate specified in the Workgroup Manager preferences. Choose the Preferences command on the Workgroup Manager menu to display the current setting for automatic refresh and optionally change it.

Finding Specific Users and Groups in a List

After you have displayed a list of users or groups in Workgroup Manager, you can filter the list to find particular users or groups of interest.

To filter items in the list of accounts:

- 1** After listing accounts, select the user or group tab.
- 2** In the pop-up menu above the account list, select an option to describe what you want to find. When you enter a name option, both full and short names of users or groups are searched. The original list is replaced by items that satisfy your search criteria.

Sorting User and Group Lists

After displaying a list of accounts in Workgroup Manager, click a column heading to sort entries using the values in that column. Click the heading again to reverse the order of the entries in the list.

Shortcuts for Working With Users and Groups

When using Workgroup Manager to work with user and group accounts, several shortcuts can save you time:

- You can make changes to multiple user or group accounts at once. See “Editing Multiple Users Simultaneously” on page 176.
- You can use presets, which are like templates that let you predefine attributes to apply to new user or group accounts by default. See “Creating a Preset for User Accounts” on page 176 through “Changing Presets” on page 178.
- You can import user and group accounts from a file. See “Understanding What You Can Import” on page 179 through “Using Character-Delimited Files” on page 187.

Editing Multiple Users Simultaneously

You can use Workgroup Manager to make the same change to multiple user accounts in a NetInfo or LDAPv3 domain at the same time.

To edit multiple users:

- 1 In Workgroup Manager, list the users in the directory domain of interest.
Click the Account button, then use the At pop-up menu to open the directory domain. Click the lock to be authenticated, then select the users in the user list. Use Command-click to select each user whose account you want to change.
- 2 Click the tab you want to work with and make changes as required for fields that Workgroup Manager lets you update.

Using Presets

Presets are Workgroup Manager account templates. They let you set up initial attributes for new accounts you create using Workgroup Manager.

Presets can be used only during account creation. If you change a preset after it has been used to create an account, accounts already created using the preset are *not* updated to reflect those changes.

Creating a Preset for User Accounts

To create a preset for user accounts:

- 1 Open Workgroup Manager on the server from which you will be creating user accounts. Ensure that the server has been configured to access the Mac OS X directory domain or non-Apple LDAPv3 directory domain in which the preset will be used to create new accounts.
- 2 Click the Accounts button.

- 3 To create a preset using data in an existing user account, open the account. To create a preset using an empty user account, create a new user account.
- 4 Fill in the fields with values you want new user accounts to inherit. Delete any values you do not want to prespecify if you are basing the preset on an existing account.

The following attributes can be defined in a user account preset: password settings, home directory settings, quotas, default shell, primary group ID, group membership list, and mail settings.

- 5 On the Presets pop-up menu, choose Save Preset, enter a name for the preset, then click OK.

Creating a Preset for Group Accounts

To create a preset for group accounts:

- 1 Open Workgroup Manager on the server from which you will be creating group accounts. Ensure that the server has been configured to access the Mac OS X directory domain or non-Apple LDAPv3 directory domain in which the preset will be used to create new accounts.
- 2 Click the Accounts button.
- 3 To create a preset using data in an existing group account, open the account. To create a preset using an empty group account, create a new group account.
- 4 Fill in the fields with values you want new user groups to inherit. Delete any values you do not want to prespecify if you are basing the preset on an existing account.
- 5 On the Presets pop-up menu, choose Save Preset, enter a name for the preset, then click OK.

Using Presets to Create New Accounts

To create a new account using a preset:

- 1 Open Workgroup Manager on a server configured to access the Mac OS X directory domain or non-Apple LDAPv3 directory domain in which the preset will be used to create the new account.
- 2 Click the Accounts button.
- 3 Use the At pop-up menu to open the directory domain in which you want the new account to reside.
- 4 Click the lock to be authenticated as a directory domain administrator.
- 5 From the Presets pop-up menu, choose the preset you want to use.
- 6 Create a new account.
- 7 Add or update attribute values as appropriate, either interactively or using an import file.

Renaming Presets

To rename a preset:

- 1 Open Workgroup Manager on the server where the preset has been defined.
- 2 Click the Accounts button.
- 3 From the Presets pop-up menu, choose Rename Preset and enter the new name.
- 4 Click OK.

Deleting a Preset

To delete a preset:

- 1 Open Workgroup Manager on the server where the preset has been defined.
- 2 Click the Accounts button.
- 3 From the Presets pop-up menu, choose Delete Preset.
- 4 Select the preset you want to delete then click Delete.

Changing Presets

When you change a preset, existing accounts created using it are not updated to reflect your changes.

To change a preset:

- 1 Open Workgroup Manager on the server where the preset has been defined.
- 2 Click the Accounts button.
- 3 From the Presets pop-up menu, choose the preset you want to change.
- 4 After completing your changes, choose Save Preset on the Presets pop-up menu.

You can also change a preset while using it to create a new account by changing any of the fields defined by the preset, then saving the preset.

Importing and Exporting User and Group Information

Importing user and group accounts from a file is useful when you want to

- Create a large number of users or groups in a batch.
- Migrate user or group accounts from another server. You can import users and groups from AppleShare IP 6.3 or Mac OS X Server version 10.1 and earlier.
- Update a large number of user or group accounts with new information.

You can import accounts into a NetInfo or LDAPv3 directory domain from

- XML files created by exporting accounts on AppleShare IP 6.3 servers.

- XML files created by exporting accounts on Mac OS X Server versions 10.1 and earlier.
- Character-delimited files created by exporting accounts on Mac OS X Server versions later than 10.1 or created by hand or using a database or spreadsheet application.

There are two ways to import and export accounts: using Workgroup Manager or using the `dsimportexport` command-line tool. `dsimportexport` gives you more control over the import and export processes, while Workgroup Manager offers a simpler, graphical user experience.

During import and export processing, `dsimportexport` displays status information and writes to a log file:

- Status information is provided for each user or group imported or exported. Status data includes the total number of records processed so far, the number of bytes processed so far, and the identity of the record being processed currently.
- The log file is created in `/Users/<user name>/Library/Logs/ImportExport/DSImportExport.logYYYY.MMDD.mmmmmm`, where `<user name>` identifies the user who invoked `dsimportexport` and `mmmmmm` is milliseconds. The log file provides both processing information and error indications. Information logged includes the date and time that the import or export operation started, the total number of users and groups imported or exported, and the identity of any accounts that generated errors during import or export.

This section describes how to prepare files for importing and how to conduct import and export operations using Workgroup Manager and `dsimportexport`.

Understanding What You Can Import

The user and group account attributes you can import vary with the kind of import file you use:

- XML files created with Mac OS X Server 10.1 or earlier (see page 186)
- XML files created with AppleShare IP 6.3 (see page 186)
- character-delimited files (see page 187)

You cannot use an import file to change these predefined users: `daemon`, `root`, `nobody`, `unknown`, or `www`. Nor can you use an import file to change these predefined groups: `admin`, `bin`, `daemon`, `dialer`, `mail`, `network`, `nobody`, `nogroup`, `operator`, `staff`, `sys`, `tty`, `unknown`, `utmp`, `uucp`, `wheel`, or `www`. You can, however, add users to the `wheel` and `admin` groups.

Using Workgroup Manager to Import Users and Groups

You can use Workgroup Manager to import user and group accounts into a NetInfo or LDAPv3 directory domain.

To import accounts using Workgroup Manager:

- 1** Create a character-delimited or XML file containing the accounts to import, and place it in a location accessible from the server on which you will use Workgroup Manager. Ensure the file contains no more than 10,000 records.

See “Using XML Files Created With Mac OS X Server 10.1 or Earlier” on page 186, “Using XML Files Created With AppleShare IP 6.3” on page 186, and “Using Character-Delimited Files” on page 187 for information on creating files to import.

- 2** In Workgroup Manager, click the Account button, then use the At pop-up menu to open the directory domain into which you want to import accounts.
- 3** Click the lock to authenticate as domain administrator.
- 4** Choose Import from the Server menu, then select the import file.
- 5** Select one of the Duplicate Handling options to indicate what to do when the short name of an account being imported matches that of an existing account.

“Overwrite existing record” overwrites any existing record in the directory domain.

“Ignore new record” ignores an account in the import file.

“Add to empty fields” merges data from the import file into the existing account when the data is for an attribute that currently has no value.

“Append to existing record” appends data to existing data for a particular multivalued attribute in the existing account. Duplicates are not created. This option might be used, for example, when importing new members into an existing group.

- 6** Select one of the Record Format options.

“Import standard users” indicates your import file contains user accounts with these attributes in the order listed: short name, password, UID, primary group ID, full name, path to the home directory on the user’s computer, and default shell. The first line of the file must contain “StandardUserRecord.”

“Import standard groups” indicates your import file contains group accounts with these attributes in the order listed: group name, group ID, and short names of group members. The first line of the file must contain “StandardGroupRecord.”

“Use record description in file” indicates that the first line of the file is a complete record description. “Using Character-Delimited Files” on page 187 describes what the record description must look like.

“Import XML from AppleShare IP” indicates your import file is an XML file created using AppleShare IP.

“Import XML from Server Admin” indicates your import file is an XML file created using Server Admin on Mac OS X Server 10.1 or earlier.

- 7 In the First User ID field, enter the UID at which to begin assigning UIDs to new user accounts for which the import file contains no UID.
- 8 In the Primary Group ID field, enter the group ID to assign to new user accounts for which the import file contains no primary group ID.
- 9 Click Import to start the import operation.

Using Workgroup Manager to Export Users and Groups

You can use Workgroup Manager to export user and group accounts from a NetInfo or LDAPv3 directory domain into a character-delimited file that you can import into a different NetInfo or LDAPv3 directory domain.

To export accounts using Workgroup Manager:

- 1 In Workgroup Manager, click the Account button, then use the At pop-up menu to open the directory domain from which you want to import accounts.
- 2 Click the lock to authenticate as domain administrator.
- 3 Choose Export from the Server menu.
- 4 Specify the name to assign to the export file and the location where you want it created.
- 5 Click Export.

Using dsimportexport to Import Users and Groups

You can use dsimportexport to import user and group accounts into a NetInfo or LDAPv3 directory domain.

Here are the parameters that dsimportexport accepts when importing user and group accounts. Parameters are delimited using angle brackets (<>) if they are required and square brackets ([]) if they are optional:

```
dsimportexport <-g or -s or -p> <file> <directoryDomain>
    <userName> <password> <O or M or I or A> <-s startingUID>
    [-r primaryGroupID] [-k keyIndex ...] [-n recNameIndex] [-v]
    [-T standardRecordType] [-yrnm userName] [-yrpwd password]
    [-y ipAddress] [-V] [-h] [-err]
```

where

-g

imports accounts from a character-delimited file. See “Using Character-Delimited Files” on page 187 for information about the format of this kind of file.

-s

imports accounts from an XML file formatted as “Using XML Files Created With Mac OS X Server 10.1 or Earlier” on page 186 describes.

-p

imports accounts from an XML file formatted as “Using XML Files Created With AppleShare IP 6.3” on page 186 describes.

file

names the file from which you want to import accounts, including the path to the file. For example, /tmp/Import1.

directoryDomain

is the full path to the NetInfo or LDAPv3 directory domain into which you want to import the accounts. For a NetInfo domain, you might type “NetInfo/root/someDomain”. For an LDAPv3 domain, an example is “LDAPv3/ldap.example.com”.

userName

is the full or short name of a user who has domain administrator privileges for the directory domain.

password

is the password associated with the userName you specify.

O

overwrites any existing record in the directory domain with the value(s) in the attribute(s) identified using the -k option.

M

merges data from the import file into an existing account, using the value(s) in the attribute(s) identified using the -k option when the data is for an attribute that currently has no value.

I

ignores an account in the import file if a record with the same value(s) in the attribute(s) identified using the -k option already exists in the directory domain.

A

appends data to existing data for a particular multivalued attribute in an account in the directory domain with the value(s) in the attribute(s) identified using the -k option. Duplicates are not created. This option might be used, for example, when importing new members into an existing group.

-s startingUID

specifies the starting UID to use when importing from an ASIP XML file or a character-delimited file that contains new user accounts with no UIDs specified. You can omit this argument if all the accounts in the import file contain UIDs, but use it if some or all of the accounts do not contain UIDs. For example, `-s 559` assigns UIDs to imported users starting at 559 and incrementing by one for each new user.

-r primaryGroupID

identifies the primary group ID to assign a new user when an account in the import file has no group ID specified. For example, `-r 20` makes the group with a group ID of 20 the primary group of an imported user with no group ID defined in the file.

-k keyIndex ...

is for character-delimited import files only. It is used to identify as many as four attributes of an account in the file that you want to use to determine whether the account already exists. The keyIndex is 0 based, so `-k 0` points to the *first* attribute of an account in the import file. Separate multiple keyIndex values using commas, for example, `-k 1,5,6,8`. If you omit the `-k` parameter, `-k 0` is assumed.

-n recNameIndex

is for character-delimited import files only. It is used to identify the attribute providing a user's short name or a group name. The nameIndex is 0 based, so `-n 0` points to the first attribute. If you omit the `-n` parameter, `-n 0` is assumed.

-v

generates verbose output during import. Because this option generates a large amount of status data for each account (including all data in the import file), use this option only when debugging import files. The default status data are counts of the number of accounts and bytes processed and the record name of the account currently being processed.

-T standardRecordType

is for character-delimited import files only. It is used to indicate that the first line of the file does not contain a record description because the file contains accounts in standard formats. A `standardRecordType` value of `xDSStandardUser` is used for standard user accounts, and `xDSStandardGroup` is used for standard group accounts. See “Using Character-Delimited Files” on page 187 for details about account formatting.

-yrnm userName

is the user name for logging in to a remote Mac OS X Server identified in the `-y` parameter.

-yrypwd password

is the password for logging in to a remote Mac OS X Server identified in the `-y` parameter.

-y ipAddress

is the IP address of a remote Mac OS X Server from which the directory domain is visible.

-V

adds the version number of dsimporlexport to the log file.

-h

displays usage information for dsimporlexport.

-err

displays error information.

To use dsimporlexport to import users and groups:

- 1 Create a character-delimited or XML file containing the accounts to import, and place it in a location accessible from the server from which you will use the tool. Ensure the file contains no more than 10,000 records.

See “Using XML Files Created With Mac OS X Server 10.1 or Earlier” on page 186, “Using XML Files Created With AppleShare IP 6.3” on page 186, and “Using Character-Delimited Files” on page 187 for information on creating files to import.
- 2 As domain administrator, log in to a server that has access to the directory domain into which you want to import accounts.
- 3 Open the Terminal application and type the dsimporlexport command. The dsimporlexport tool is located in /usr/sbin.

Using dsimporlexport to Export Users and Groups

You can use dsimporlexport to export user and group accounts from NetInfo or LDAPv3 directory domains into a character-delimited file that you can import into a different Mac OS X or non-Apple LDAPv3 directory domain.

Here are the parameters that dsimporlexport accepts when exporting user and group accounts. Parameters are delimited using angle brackets (<>) if they are required and square brackets ([]) if they are optional:

```
dsimporlexport -x <file> <directoryDomain>  
    [-v] [-d delimiter ...] [-yrnm userName]  
    [-yrpwd password] [-y ipAddress] [-V] [-h] [-err]
```

where

-x

exports accounts into a character-delimited text file. See “Using Character-Delimited Files” on page 187 for information about the format of this kind of file.

file

names the file to which you want to export accounts, including the path to the file. For example, /tmp/Export1. The file should not already exist.

directoryDomain

is the full path to the NetInfo or LDAPv3 directory domain from which you want to export the accounts. For a NetInfo domain, you might type “NetInfo/root/someDomain”. For an LDAPv3 domain, an example is “LDAPv3/ldap.example.com”.

-v

generates verbose output during export. Because this option generates a large amount of status data for each account (including all data in the export file), use this option only when debugging export files. The default status data are a count of the number of accounts processed and the record name of the account currently being processed.

-d delimiter

is for character-delimited export files only. This parameter specifies four delimiters in this order: end of record, escape, end of field, and end of value. The delimiters values must be expressed using hex strings, for example, 0x0A. If you omit this parameter, the default delimiters are \n (end of record, 0x0A), \ (escape, 0x5C), : (end of field, 0x3A), and , (end of value, 0x2C).

-yrnm userName

is the user name for logging in to a remote Mac OS X Server identified in the -y parameter.

-yrypwd password

is the password for logging in to a remote Mac OS X Server identified in the -y parameter.

-y ipAddress

is the IP address of a remote Mac OS X Server from which the directory domain is visible.

-V

adds the version number of dsimportexport to the log file.

-h

displays usage information for dsimportexport.

-err

displays error information.

To use dsimportexport to export users and groups:

- 1 As domain administrator, log in to a server that has access to the directory domain from which you want to export accounts.

- 2 Open the Terminal application and type the `dsimportexport` command. The `dsimportexport` tool is located in `/usr/sbin`.

Using XML Files Created With Mac OS X Server 10.1 or Earlier

You can use Server Admin to create an export file from Mac OS X Server versions 10.1 or earlier, and import that file into a NetInfo or LDAPv3 directory domain using Workgroup Manager or `dsimportexport`.

The following user account attributes are exported into these XML files. Attributes in angle brackets (`<>`) are required and will generate an error if absent when you use the file as an import file:

- indication of whether user can log in
- indication of whether user is a server administrator
- `<UID>`
- `<primary group ID>`
- shell
- comment
- `<short name>`
- `<full name>`
- `<password format>` and `<password text>`.
- Apple mail data
- ara (Apple Remote Access; this data is ignored.)

The following group account attributes might be present in these XML files:

- `<group name>`
- `<group ID>`
- `<one member's short name>`
- other members' short names

Using XML Files Created With AppleShare IP 6.3

You can use the Web & File Admin application to create an export file on an AppleShare IP 6.3 server and import that file into a NetInfo or LDAPv3 directory domain using Workgroup Manager or `dsimportexport`.

The following user account attributes are exported into these XML files. Attributes in angle brackets (`<>`) are required and will generate an error if absent when you use the file as an import file:

- `<name>` (mapped to a full name)
- `inetAlias` (mapped to a short name)

- comment
- indication of whether user can log in
- <password format> and <password text>.
- Apple mail data
- indicator for whether the user is a server administrator, password change data, and indicator for forcing a password to change (this data is ignored)

The dsimportexport tool generates UIDs when you import this XML file, using the -s parameter to determine the UID to start with and incrementing each subsequently imported account's UID by one. It generates primary group IDs using the -r parameter. When you import using Workgroup Manager, UIDs and primary group IDs are generated as you indicate in the dialog box provided.

The following group account attributes might be present in these XML files:

- <group name>
- <one member's short name>
- other members' short names

dsimportexport generates group IDs when you import this XML file, using the -r parameter to determine the group ID to start with and incrementing each subsequently imported group's ID by one. When you import using Workgroup Manager, group IDs are generated using the information you provide for primary group IDs in the import dialog box.

Using Character-Delimited Files

You can create a character-delimited file by using Workgroup Manager or dsimportexport to export accounts in NetInfo or LDAPv3 directory domains into a file. You can also create a character-delimited file by hand or by using a database or spreadsheet application.

The first record in the file must characterize the format of each account in the file. There are three options:

- Write a full record description.
- Use the shorthand "StandardUserRecord."
- Use the shorthand "StandardGroupRecord."

The other records in the file describe user or group accounts, encoded in the format described by the first record.

Any line of a character-delimited file that begins with "#" is ignored during importing.

Writing a Record Description

A record description identifies the fields in each record you want to import from a character-delimited file; indicates how records, fields, and values are separated; and describes the escape character that precedes special characters in a record. Encode the record description using the following elements in the order specified, separating them using a space:

- End-of-record indicator (in hex notation)
- Escape character (in hex notation)
- Field separator (in hex notation)
- Value separator (in hex notation)
- Type of accounts in the file (DSRecTypeStandard:Users or DSRecTypeStandard:Groups)
- Number of attributes per account
- List of attributes

For user accounts, the list of attributes must include the following, although you can omit UID and PrimaryGroupID if you specify a starting UID and a default primary group ID when you import the file:

- RecordName (the user's short name)
- Password
- UniqueID (the UID)
- PrimaryGroupID
- RealName (the user's full name)

In addition, you can include

- UserShell (the default shell)
- NFSHomeDirectory (the path to the user's home directory on the user's computer)
- Other user attributes, described in Appendix A

For group accounts, the list of attributes must include

- RecordName (the group name)
- PrimaryGroupID (the group ID)
- GroupMembership

In addition, you can include other user attributes, described in Appendix A.

Here is an example of a record description:

```
0x0A 0x5C 0x3A 0x2C DSRecTypeStandard:Users 7  
RecordName Password UniqueID PrimaryGroupID  
RealName NFSHomeDirectory UserShell
```

Here is an example of a record encoded using the description:

```
jim:Adl47E$:408:20:J. Smith, Jr., M.D.:/Network/Servers/somemac/Homes/jim:/bin/csh
```

Using the StandardUserRecord Shorthand

When the first record in a character-delimited import file contains “StandardUserRecord,” the record description assumed is

```
0x0A 0x5C 0x3A 0x2C DSRecTypeStandard:Users 7
RecordName Password UniqueID PrimaryGroupID
RealName NFSHomeDirectory UserShell
```

An example user account looks like this:

```
jim:Adl47E$:408:20:J. Smith, Jr., M.D.:/Network/Servers/somemac/Homes/jim:/bin/csh
```

Using the StandardGroupRecord Shorthand

When the first record in a character-delimited import file contains “StandardGroupRecord,” the record description assumed is

```
0x0A 0x5C 0x3A 0x2C DSRecTypeStandard:Groups 4
Record Name PrimaryGroupID GroupMembership
```

Here is an example of a record encoded using the description:

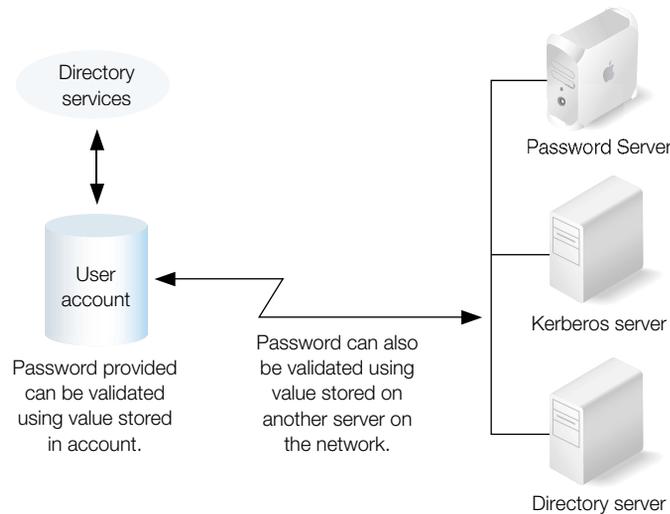
```
students:Ad147:88:jones,thomas,smith,wong
```

Understanding Password Validation

A user’s password can be validated using one of these options:

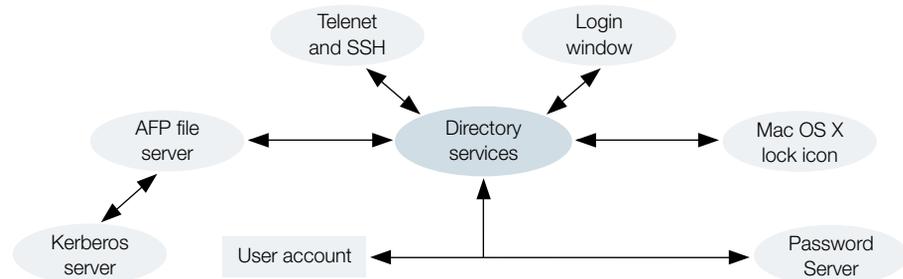
- Using a value stored as a readable attribute in the user’s account. The account can be stored in a directory domain residing on Mac OS X Server or on another vendor’s directory server, such as an LDAP or Active Directory server.
- Using a value stored in the Open Directory Password Server.
- Using a Kerberos server.

- Using LDAP bind authentication with a non-Apple LDAPv3 directory server.



Clients needing password validation, such as login window and the AFP server, call Mac OS X directory services. Directory services determines from the user's account how to validate the password.

- Directory services can validate a password stored in the account or by interacting with the Password Server or a remote LDAP directory server (using LDAP bind authentication).
- If a Kerberos server is used to validate a user, when the user accesses a Kerberized client, such as the AFP server in the following picture, the client interacts directly with the Kerberos server to validate the user. Then the client interacts with directory services to retrieve the user's record for other information it needs, such as the UID or primary group ID.



See "The Authentication Authority Attribute" on page 192 for information about the attribute in a user's account that indicates how to validate a particular user's password.

Contrasting Password Validation Options

Here are the pros and cons of the options for validating a user's password:

- Storing a password in the user's account. This approach, referred to as the "basic" password validation strategy, is the default strategy. It is the simplest and fastest strategy, since it does not depend on another infrastructure for password validation. It is the strategy most compatible with software that needs to access user records directly, such as legacy UNIX software. It supports users logging in to computers running Mac OS X version 10.1 and earlier as well as Windows users authenticated using Authentication Manager when they log in to a Mac OS X Server version 10.1.

When integrating with existing directory systems, such as LDAP and Active Directory servers, this strategy offers the greatest opportunity for both Mac OS X Server and the directory server to use the same record to authenticate a user who wants to use that server.

This strategy may not support clients that require certain network-secure authentication protocols (such as SMB, APOP, or CRAM-MD5) when transmitting passwords to a particular service. Also, this strategy can make your server vulnerable to offline attacks, since readable versions of passwords are used. See "The Problem With Readable Passwords" on page 194 for more information about offline attacks.

See "Storing Passwords in User Accounts" on page 193 for details about this strategy.

- Using a Password Server. This strategy lets you set up user-specific password policies for users. You can require a user to change his password periodically or use only passwords having more than a minimum number of characters. It supports clients that can use basic authentication as well as clients requiring network-secure authentication protocols that protect the privacy of a password during transmission. It is the recommended method to use for Windows clients. It is the only way to authenticate AFP clients prior to version 3.8.3, because they require AFP 2-Way Random authentication, which Password Server supports.

Password Server passwords can't be used during login to computers running Mac OS X version 10.1 or earlier. In addition, this strategy relies on the availability of a Password Server on a Mac OS X Server; if the Password Server goes down, password validation cannot occur, because you cannot replicate a Password Server. Also, you must ensure that physical access to the server on which Password Server resides is controlled.

See "Using a Password Server" on page 195 for details about this strategy.

- Using a Kerberos server. This option is not supported by all services but offers the opportunity to integrate into existing Kerberos environments. As in the case of the Password Server, if the Kerberos server is unavailable, users whose passwords are verified using it are unable to use your server.

See "Using Kerberos" on page 197 for details about this strategy.

- Using an LDAP server. This option, like Kerberos, offers a way to integrate your Mac OS X Server into an existing authentication scheme.
See “Using LDAP Bind Authentication” on page 201 for details about this strategy.

The Authentication Authority Attribute

To authenticate a user, Mac OS X directory services first locates the user’s record using the user name provided by the user. Then it determines which password validation scheme to use by consulting the “authentication authority” attribute in the user’s account.

The authentication authority attribute identifies the password validation scheme and provides additional information as required. For example, if a Password Server is being used, the location of the Password Server is part of the authentication authority value.

If a user’s account contains no authentication authority attribute, the basic strategy is used. For example, user accounts created using Mac OS X version 10.1 and earlier contain no authentication authority attribute.

Choosing a Password

The password associated with a user’s account must be entered by the user before he or she can be authenticated. The password is case-sensitive (except for SNB LAN Manager passwords) and does not appear on the screen as it is entered.

Regardless of the password validation option you use for any user, here are some guidelines for composing a password for Mac OS X Server users.

A password should contain 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.) A zero-length password is not recommended, and some systems (such as LDAP bind) do not allow them.

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 information to determine whether you need to take these restrictions into account when defining passwords for server users:

- Apple file service accepts 7-bit or 8-bit ASCII passwords.
- File Transfer Protocol (FTP) service accepts 7-bit ASCII passwords.
- IMAP accepts 7-bit ASCII passwords. Some IMAP clients accept 8-bit ASCII passwords.
- Macintosh Manager accepts 7-bit or 8-bit ASCII passwords.
- POP3 accepts 7-bit ASCII passwords.
- Web service accepts 7-bit ASCII passwords.

- Windows service accepts 7-bit ASCII passwords.
- Server Settings accepts 7-bit or 8-bit ASCII passwords.

Migrating Passwords

When you import user accounts from computers running Mac OS X Server version 10.1 or earlier, no authentication authority attribute exists. Therefore all these users have basic password validation enabled initially. When importing users from servers supporting Windows users, Authentication Manager passwords may have been used to set the passwords.

While all the existing passwords can continue to be used after importing the users, if you want to use the Password Server for imported users, you'll need to reset their passwords after importing them. "Enabling the Use of a Password Server for a User" on page 196 describes how to change a basic password to a Password Server password.

Setting Up Password Validation Options

The sections that follow describe how to set up the different kinds of password validation for individual users:

- To store a password in a user's account, see "Storing Passwords in User Accounts" on page 193.
- To use a Password Server to validate a user's password, see "Enabling the Use of a Password Server for a User" on page 196.
- To use a Kerberos server, see "Integrating Mac OS X With a Kerberos Server" on page 199.
- To use LDAP bind authentication, see "Using LDAP Bind Authentication" on page 201.

Storing Passwords in User Accounts

This password management strategy is the default strategy, but cannot be used to validate the passwords of clients that require network-secure authentication protocols. (The single exception is users created using Mac OS X Server version 10.1 in NetInfo domains with Authentication Manager enabled.) Use the Password Server if you need to support these kinds of client computers.

Enabling Basic Password Validation for a User

Basic password validation is the simplest form of password validation. It relies on a readable version of a user's password, stored in the user account. Only the first 8 characters are used for password validation.

A user's password is stored in the user account in an encrypted form, derived by feeding a random number along with the clear text password to a mathematical function, known as a one-way hash function. A one-way hash function always generates the same encrypted value from particular input, but cannot be used to re-create the original password from the encrypted output it generates.

To validate a password using the encrypted value, Mac OS X applies the function to the password entered by the user and compares it with the value stored in the user account. If the values match, the password is considered valid.

You can use Workgroup Manager to enable using the basic password validation strategy for user accounts stored in a Mac OS X directory or non-Apple LDAPv3 directory domain.

To enable basic password validation using Workgroup Manager:

- 1** In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. Click the lock to be authenticated, then select the user in the list.
- 2** On the Advanced tab, choose Basic from the "Use Password Type" pop-up menu.
- 3** If the user's password validation strategy is currently a different one, you will be prompted to enter and verify a new password.

If you are working with a new user, enter the password on the Basic tab in the Password field, then reenter it in the Verify field. "Choosing a Password" on page 192 provides guidelines for choosing passwords.

The Problem With Readable Passwords

Whenever you store passwords in a readable form, they are potentially subject to hacking.

Consider, for example, NetInfo user records. Although the passwords in NetInfo user records are encrypted using one-way encryption, they are readable because the `nidump` utility can be used to copy user records to a file. The file can be transported to a system where a malicious user can use various techniques to figure out which password values generate the encrypted values stored in the user records.

This form of attack is known as an offline attack, since it does not require successive login attempts to gain access to a system. As soon as a password is identified, the correct user name and password can be supplied and the malicious user can log in successfully without notice.

Using a Password Server

The Password Server stores passwords, but never allows passwords to be read. Passwords can only be set and verified. Malicious users must log in over the network to attempt to gain system access, and invalid password instances, logged by the Password Server, can alert you to such attempts.

The Password Server is based on a standard known as SASL (Simple Authentication and Security Layer). This approach helps it support a wide range of network user authentication protocols that are used by clients of Mac OS X Server services, such as mail and file servers, that need to authenticate users. Some of the protocols also support clients that require clear text or unique hashes. Here are a few of the network authentication protocols that the Password Server supports:

- CRAM-MD5
- MD5
- APOP
- NT and LAN Manager (for SMB)
- SHA-1
- DHX
- AFP 2-Way Random
- WebDAV Digest

The account for a user whose password is validated using the Password Server does not store the user's password. Instead, it stores—in its authentication authority attribute—a unique password ID, assigned by the Password Server when the account was set up to use the Password Server. To validate a password, directory services passes the password ID to the Password Server, which it locates using its network address, also stored in the authentication authority attribute. The Password Server uses the password ID as a key for finding the actual password and any associated password policy.

For example, the Password Server may locate a user's password, but discover that it has expired. If the user is logging in, login window presents the user with a dialog box for changing the password. After providing a new password, the user can be authenticated.

The Password Server maintains a record for each user that includes

- The password ID, a 128-bit value assigned when the password is created. The value includes a key for finding a user's password record.
- The password, stored in recoverable or hashed form. The form depends on the network authentication protocols enabled for the Password Server (using Open Directory Assistant). If APOP or 2-way Random is enabled, the Password Server stores a recoverable (encrypted) password. If neither of these methods is enabled, only hashes of the passwords are stored.

- Data about the user that is useful in log records, such as the short name.
- Password policy data.

Setting Up a Password Server

The account for a user validated using the Password Server is stored in a NetInfo or LDAPv3 directory domain that resides on Mac OS X Server. Before you set up a user's account to use a Password Server, you need to set up the Password Server.

See Chapter 2, "Directory Services," for instructions on how to set up a Password Server. It describes how to use Open Directory Assistant to

- create a Password Server
- associate a directory domain with a Password Server
- designate an administrator for the Password Server

Any user you designate to be an administrator for the Password Server becomes the domain administrator for the directory domain with which the server is associated. This administrator's password is validated using that Password Server, so that the administrator is able to update passwords for user accounts that use that Password Server.

Enabling the Use of a Password Server for a User

Use Workgroup Manager to enable the use of a Password Server for validating passwords for user accounts stored in a NetInfo or LDAPv3 directory domain residing on Mac OS X Server.

To enable the use of a Password Server for a user:

- 1** Make sure a Password Server has been associated with the directory domain in which the user's account resides.
- 2** In Workgroup Manager, open the account you want to work with if it is not already open.
To open an account, click the Account button, then use the At pop-up menu to open the directory domain where the user's account resides. Click the lock to be authenticated, then select the user in the list.
- 3** On the Advanced tab, choose "Password Server" from the "Use Password Type" pop-up menu.
- 4** If the user's password is currently being validated using a different strategy, you will be prompted to enter and verify a new password. If you are working with a new user, enter the password on the Basic tab in the Password field, then reenter it in the Verify field. The password must contain no more than 512 characters, although there may be different limits imposed by the network authentication protocol; for example, 128 characters for SMB NT, 14 for SMB LAN Manager, 8 for AFP 2-way random, and 8 for Crypt (basic). "Choosing a Password" on page 192 provides guidelines for choosing passwords.

- 5 On the Advanced tab, click Options to set up the user's password policy. Click OK when you are done.

The password ID is a unique 128-bit number assigned when the password is created on the Password Server. It may be helpful in troubleshooting, since it appears in the Password Server log when a problem occurs. View this log in the directory services section of Server Status.

Exporting Users With Password Server Passwords

The Password Server does not let you read passwords. Therefore when you export user accounts that have Password Server passwords, passwords are not exported.

When you import such users, you must reset all their passwords after importing their accounts. “Enabling the Use of a Password Server for a User” on page 196 describes how.

Making a Password Server More Secure

Using a Password Server offers flexible and secure password validation, but you need to make sure that the server on which a Password Server runs is secure:

- Set up Password Servers on a server that is not used for any other activity.
- Since the load on a Password Server is not particularly high, you can have several (or even all) of your server-resident directory domains share a single Password Server.
- Make sure that the Password Server's computer is located in a physically secure location.

Monitoring a Password Server

Use the Password Server logs, visible using Server Status, to monitor failed login attempts.

Password Server logs all failed authentication attempts, including IP addresses that generate them. Periodically review the logs to determine whether there are a large number of failed trials for the same password ID, indicating that somebody may be generating login guesses.

Using Kerberos

If you already use Kerberos to authenticate users, you can use Kerberos to validate passwords for the following services of Mac OS X Server version 10.2 and later:

- Login window
- Mail service
- FTP
- AFP server and client

- Telnet server

These services have been “Kerberized.” Only services that have been Kerberized can use Kerberos to validate a user.

Understanding Kerberos

Like the Password Server, a Kerberos server is dedicated to handling data needed for user validation. Other user data is maintained in a separate server.

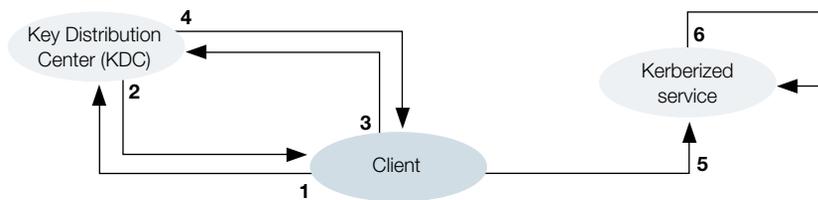
Kerberized services are configured to authenticate principals who are known to a particular Kerberos realm. You can think of a “realm” as a particular Kerberos database or authentication domain, which contains validation data for users, services, and sometimes servers (known as “principals”). For example, a realm contains principals’ private keys, which are the result of a one-way function applied to passwords. Service principals are generally based on randomly generated secrets rather than passwords.

Here are examples of realm and principal names; note that realm names are capitalized by convention to distinguish them from DNS domain names:

- Realm: MYREALM.EXAMPLE.COM
- User principal: smitty@MYREALM.EXAMPLE.COM
- Service principal: afpserver/anothername.example.com@MYREALM.EXAMPLE.COM

There are several phases to Kerberos authentication. In the first phase, the client obtains credentials to be used to request access to Kerberized services. In the second phase, the client requests authentication for a specific service. In the final phase, the client presents those credentials to the service.

The following illustration summarizes these activities. Note that the service and the client in this picture may be the same entity (such as login window) or two different entities (such as a mail client and the mail server).



- 1 The client authenticates to a Kerberos Key Distribution Center (KDC), which interacts with realms to access authentication data. This is the only step in which passwords and associated password policy information needs to be checked.
- 2 The KDC issues the client a ticket-granting ticket, the credential needed when the client wants to use Kerberized services. the ticket-granting ticket is good for a configurable period of time, but can be revoked before expiration. It is cached on the client until it expires.

- 3 The client contacts the KDC with the ticket-granting ticket when it wants to use a particular Kerberized service.
 - 4 The KDC issues a ticket for that service.
 - 5 The client presents the ticket to the service.
 - 6 The service verifies that the ticket is valid. If the ticket is valid, usage of the service is granted to the client if the client is authorized to use the service. (Kerberos only authenticates clients; it does not authorize them to use services. An AFP server, for example, needs to consult a user's account in a directory domain to obtain the UID.) The service uses information in the ticket if required to retrieve additional information about the user from a directory domain.
- Note that the service does not need to know any password or password policy information. Once a ticket-granting ticket has been obtained, no password information needs to be provided.

For more information on Kerberos, go to the MIT Kerberos home page:
web.mit.edu/kerberos/www/index.html

Integrating Mac OS X With a Kerberos Server

To integrate Mac OS X with a Kerberos server:

- 1 Make sure that one or more realms supported by your Kerberos server contain information for all the users to be validated using Kerberos and for all the Mac OS X Kerberized services they will use. The Kerberos principal name must be the same as the short name in the user's directory domain account.
- 2 Create user accounts for each of the same users in directory domains accessible from Mac OS X computers on which Kerberized services will be used. Set the password type to Basic, and specify passwords that will never be used to authenticate the users.

Kerberized services on Mac OS X computers retrieve user accounts by extracting the user name part of the principal out of the KDC certificate, which is passed to directory services to find the account.

- 3 Before enabling Kerberos for a specific Kerberized service, create one or more principals in the KDC for it, save the shared secrets into a keytab file, and copy the keytab file from the KDC to `/etc/krb5.keytab` on your Mac OS X Server.

Use the `kadmin` command-line tool to create principals and a keytab file, and use a file sharing protocol to transfer the keytab file from the Kerberos server to Mac OS X Server. FTP or SCP (secure copy over SSH) are most likely to be present on the KDC.

Keytab files are sensitive, because they contain information used to determine whether a client or service is trustworthy.

- 4 On Mac OS X Server, place the edu.mit.Kerberos configuration file in /Library/Preferences/. This file is not sensitive, so it can be placed on a guest-accessible volume.
This file must also reside in /Library/Preferences/ in the home directory of users you want to authenticate using Kerberos.
- 5 Enable individual services (mail, AFP, and FTP) and clients (login window, AFP client, mail client) to support Kerberos authentication.
- 6 Make sure that users you want authenticated using Kerberos are in the search path of the server hosting the Kerberized services.

Enabling Kerberos Authentication for Mail

Use Server Settings to enable mail server support for Kerberos. See “Requiring or Allowing Kerberos Authentication” on page 381 for details.

To enable mail client support, set up Mac OS X Mail application account preferences to use Kerberos V5 authentication. Also make sure that edu.mit.Kerberos resides in /Library/Preferences/ on the user’s computer.

Enabling Kerberos Authentication for AFP

Use Server Settings to enable AFP server support for Kerberos. See Chapter 5, “File Services,” for details.

AFP client has no special requirements beyond access to /Library/Preferences/edu.mit.Kerberos.

Enabling Kerberos Authentication for FTP

Use Server Settings to enable FTP server support for Kerberos. See Chapter 5, “File Services,” for details.

Enabling Kerberos Authentication for Login Window

In addition to access to /Library/Preferences/edu.mit.Kerberos, login window depends on these settings in /etc/authorization:

```
<key>system.login.done </key>
<dict>
  <key>eval </key>
  <string>switch_to_user,krb5auth:login </string>
</dict>
```

Enabling Kerberos Authentication for Telnet

To set up Telnet support, edit the `/etc/inetd.conf` file to enable Telnet.

Solving Problems With Kerberos

See “Kerberos Users Can’t Authenticate” on page 204 for troubleshooting tips.

Using LDAP Bind Authentication

When you use this password validation technique, you rely on an LDAPv2 or LDAPv3 server to authenticate a user’s password. Because it supports the Secure Socket Layer (SSL) protocol, LDAPv3 is preferred.

You can use Workgroup Manager to enable the use of LDAP bind authentication for user accounts stored in a NetInfo or LDAPv3 directory domain.

To enable LDAP bind user authentication using Workgroup Manager:

- 1 Make sure the account for a user whose password you want to validate using LDAP bind resides on an LDAPv3 server in the search path of the Mac OS X computer that needs to validate the password.

See Chapter 2, “Directory Services,” for information about configuring LDAPv3 server connections. Avoid mapping the password attribute when configuring the connection; bind authentication will occur automatically. Also, set up the connection so it uses SSL in order to protect the password, passed in clear text, while it is in transit.

- 2 In Workgroup Manager, open the account you want to work with if it is not already open. To open an account, click the Account button, then use the At pop-up menu to open the LDAPv3 directory domain where the user’s account resides. Click the lock to be authenticated, then select the user in the user list.
- 3 On the Advanced tab, choose Basic from the “Use Password Type” pop-up menu.
- 4 On the Basic tab, make sure the Password field is empty.

Backing Up and Restoring Files

Regularly back up your Password Server as well as your root and administrator user accounts.

Backing Up a Password Server

Back up your Password Server frequently. When you do so, also back up any directory domain(s) that use the Password Server:

- To back up a Password Server, back up these two files: `/var/db/authserver/authservermain` and `/var/db/authserver/authserverfree`. Make sure that your Password Server backup files are as carefully secured as the computer hosting your Password Server.
- See Chapter 2, “Directory Services,” for information on backing up directory domains.

If you restore the Password Server, make sure you also restore the corresponding directory domains at the same time.

Backing Up Root and Administrator User Accounts

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 recreate these user IDs, periodically export the server’s user and group information to a file as “Importing and Exporting User and Group Information” on page 178 describes.

Supporting Client Computers

Validating Windows User Passwords

Using the Password Server is recommended for validating passwords of Windows users supported by your server.

Windows users supported by Mac OS X Server 10.1 and earlier were optionally authenticated using Authentication Manager, which offered encrypted password support. If you export users such as these and import them, Basic password validation is assumed and the Authentication Manager information is lost. You need to reset the passwords for such users before they can be used with certain network protocols.

Setting Up Search Policies on Mac OS X Client Computers

Mac OS X client computer search policies must be set up so that accounts and shared resources (such as network file servers and printers) are visible from the Mac OS X computer. See Chapter 2, “Directory Services,” for client configuration options and instructions.

Solving Problems

Follow the suggestions in this section when problems with user and group account administration arise.

You Can’t Modify an Account Using Workgroup Manager

Before you can modify an account using Workgroup Manager:

- You must be a domain administrator for any Apple directory domain storing the account.
- The directory domain must be a NetInfo or LDAPv3 directory domain. Only these domains can be updated using Workgroup Manager.

A Password Server User's Password Can't Be Modified

Before you can modify the password of a user whose password is validated using a Password Server, you must

- be a domain administrator for the directory domain storing the user's account
- have your own password validated by the same Password Server

Users Can't Log In or Authenticate

Try these techniques to determine whether the source of the authentication problem is configuration or the password itself:

- Reset the password to a known value, then determine whether there is still a problem. Try using a 7-bit ASCII password, which is supported by most clients.
- If a Password Server is being used for the user and it is not set up to support the authentication protocol needed by the user's client, you can use Open Directory Assistant to enable additional Password Server protocols. You may need to reset the user's password after changing the Password Server configuration.
- Basic authentication does not support many authentication protocols. To increase the possibility that a user's client applications will be supported, use the Password Server or suggest that the user try a different application.
- For Kerberos troubleshooting tips, see "Kerberos Users Can't Authenticate" on page 204.
- If a Password Server or non-Apple directory server used for password validation is not available, reset the user's password to use a server that is available.
- Make sure that the password contains characters supported by the authentication protocol. Leading, embedded, and trailing spaces as well as special characters (for example, option-8) are not supported by some protocols. For example, leading spaces work over POP or AFP, but not over IMAP.
- Make sure that the keyboard being used by the user supports the characters necessary for authentication.
- Make sure the client software encodes the password so that it is recognized correctly. For example, Password Server recognizes UTF-8 encoded strings, which may not be sent by some clients.
- Make sure that the client being used by the user supports the password length. For example, LAN Manager only supports 14-character passwords, so passwords longer than 14 characters would cause an authentication failure even though Mac OS X Server's Windows service supports longer passwords.

- If an AFP client prior to version 3.8.3 fails to authenticate, use AFP 2-Way Random authentication in Password Server for these older clients.

You Can't Assign Server Administrator Privileges

In order to assign server administrator privileges to a user for a particular server, first log in to that server in Workgroup Manager.

Users Can't Access Their Home Directories

Make sure 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.

Mac OS X User in 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.

Kerberos Users Can't Authenticate

When a user or service that uses Kerberos experiences authentication failures, try these techniques:

- Kerberos behavior is based on encrypted timestamps. If there's more than 5 minutes difference between the KDC, client, and service computers, authentication may fail. Make sure that the clocks for all computers are synchronized using a network time server.
- If Kerberos is being used, make sure that Kerberos authentication is enabled for the service in question.
- If a Kerberos server used for password validation is not available, reset the user's password to use a server that is available.
- Make sure that the server providing the Kerberized service has access to directory domains containing accounts for users who are authenticated using Kerberos. One way to do this is to use a shared directory domain on the KDC server that hosts user records that correspond to all the user principals.
- Refer to the KDC log (kdc.log) for information that can help you solve problems. Incorrect setup information such as wrong configuration file names can be detected using the logs.
- Make sure all your configuration files are complete and correct. For example, make sure the keytab file on your server has the principals of interest in it.

Sharing

The Sharing module of Workgroup Manager lets you share information with clients of the Mac OS X Server and control access to shared information by assigning access privileges.

You share information by designating share points. A *share point* is a folder, hard disk (or hard disk partition), or CD that you make 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 their desktops, and as volumes in the Finder in Mac OS X.

Setting up share points and assigning privileges is an integral part of setting up file services. See Chapter 5, "File Services."

Privileges

Privileges define the kind of access users have to shared items. 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).

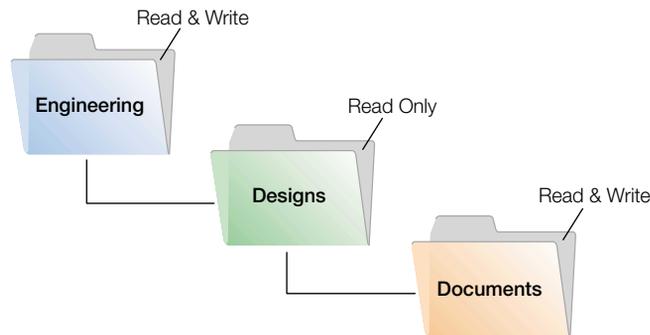
Users can	Read & Write	Read Only	Write Only	None
Open a shared file	Yes	Yes	No	No
Copy a shared file	Yes	Yes	No	No
Open a shared folder or share point	Yes	Yes	No	No
Copy a shared folder or share point	Yes	Yes	No	No
Edit a shared file's contents	Yes	No	No	No
Move items into a shared folder or share point	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 the drop box, without seeing what it contains.

Note: QuickTime Streaming Server and WebDAV have their own privileges settings. For information about QTSS, refer to the QTSS online help and the QuickTime Web site (www.apple.com/quicktime/products/qtss/). You'll find information on Web privileges in "Understanding WebDAV" on page 339.

Explicit Privileges

Share points and the shared items contained in share points (including both folders and 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:



When new files and folders are created, however, they inherit the privileges of their parent folder. See "Privileges in the Mac OS X Environment" on page 207.

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. By default, the *owner* of an item and the server administrator are the only users who can change its access privileges—allow a group or everyone to use the item. The administrator can also transfer ownership of the shared item to another user.

Note: When you copy an item to a drop box on an Apple file server, ownership of that item is transferred to the owner of the drop box. This is done because only the owner of the drop box has access to items copied to it.

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 of AppleShare Client software can set access privileges for files and folders they own. Windows file sharing users can set folder properties, but not privileges.

Privileges in the Mac OS X Environment

If you are new to Mac OS X and are not familiar with UNIX, it is important to know that there are some differences from the Mac OS 9 environment in how ownership and privileges are handled.

To increase security and reliability, Mac OS X sets many system directories, such as /Library, to be owned by the root user. Files and folders owned by root can't be changed or deleted by you unless you are logged in as the root user. Be careful when you log in as the root user since changing system data can cause problems.

As mentioned above, files and folders are, by default, owned by the user who created them. They inherit the privileges of the folder in which they are created. After they are created items keep their privileges even when moved, unless the privileges are explicitly changed by their owners or an administrator.

Therefore new files and folders you create are not accessible by client users if they are created in a folder for which the users do not have privileges. When setting up share points, make sure that items allow appropriate access privileges for the users with whom you want to share them.

Network Globe Contents

You can customize the directory structure and contents of the Network Globe for clients by setting up automounting for share points. You can add system resources such as fonts and preferences by automounting share points in specific directory locations.

Share Points in the Network Globe

The Network globe on OS X clients represents the Darwin /Network directory. By default, the Network globe contains the following four folders:

- Applications
- Library
- Servers
- Users

You can mount share points into any of these folders. See “Automounting Share Points” on page 214 for instructions.

Static Versus Dynamic Linking

Share points can be automounted statically or dynamically. Statically mounted share points are mounted when the client computer starts up. A connection to the server is opened for static mounts during startup and remains open until the user shuts down the computer. Dynamically mounted share points are not mounted until the user opens the directory. Although an icon for the directory appears in the Network globe during startup, the actual connection to the server where the directory resides is not made until the user selects the icon and attempts to access the directory’s contents.

In both cases, when an automounted share point is defined on the server it is not available to a client computer until the client has restarted.

Adding System Resources to the Network Library Folder

This Library folder in the Network globe is included in the system search path. This gives you the ability to make available, from the network, any type of system resource that resides in the local Library folder. These resources could include fonts, application preferences, ColorSync profiles, desktop pictures, and so forth. OS X accesses the network Library folder before the local Library folder, so network resources with the same name take precedence. You can use this capability to customize your managed client environment.

For example, suppose you wish to have a specific set of fonts available to each user in a given Open Directory domain. You would create a share point containing the desired fonts and then set the share point to automount into the /Network/Library/Fonts folder on client machines. See “Automounting Share Points” on page 214 for instructions on setting up automounting.

Setup Overview

You use the Sharing module of Workgroup Manager to create share points and set privileges for them.

Here is an overview of the basic steps for setting up sharing:

Step 1: Read “Before You Begin”

Read “Before You Begin” on page 209 for issues you should consider before sharing information on your network.

Step 2: Locate or create the information you want to share

Decide which volumes, partitions, folders, and CDs you want to share. You may want to move some folders and files to different locations before setting up sharing. 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. See “Organize Your Shared Information” on page 210.

Step 3: Designate share points and set privileges

When you designate an item to be a share point, you set its privileges at the same time. You create share points and set privileges in the Sharing module of Workgroup Manager. See “Setting Up Sharing” on page 211.

Step 4: Turn file services on

In order for users to be able to access share points, you must turn on the Mac OS X Server file services. Turn on each file service that you use to share items. For example, if you use Apple File Protocol with your share point, you must turn on Apple File Server. You can share an item using more than one protocol. See Chapter 5, “File Services,” on page 221.

Before You Begin

Before you assign privileges, you need to understand how privileges for shared items work. Consider which users need access to shared items and what type of privileges you want those users to have. Privileges are described at the beginning of this chapter—see “Privileges” on page 205.

You also need to determine which protocols clients will use to access share points. In general, you will want to set up independent share points for each type of client, and share the item using a single protocol:

- Mac OS clients—Apple Filing Protocol (AFP)
- Windows clients—Server Message Block (SMB)
- FTP clients—File Transfer Protocol (FTP)
- UNIX clients—Network File System (NFS)

In some cases you will want to share an item using more than one protocol. If client users will be sharing files that have common formats across platforms, you will want to create a share point that supports users of each platform. For example, Mac OS and Windows users might want to share graphics or word processing files that can be used on either platform.

Conversely, you might want to set up share points using a single protocol even though you have different kinds of clients. For example, if almost all of your clients are UNIX users and just a couple are Mac OS clients, you may want to share items using only NFS in order to keep your setup simple. Keep in mind, however, that Mac OS users will not enjoy the features of AFP not provided by NFS, such as the ability to search server contents using Sherlock, and performance optimization.

See Chapter 5, “File Services,” on page 221 for more information.

Organize Your Shared Information

Once you have created share points, users will start to form “mental maps” of the share points you have set up and the items contained in them. Changing share points and moving information around could cause confusion. If you can, organize the information you share before you start creating share points. This is especially important if you are setting up network home directories (see “Administering Home Directories” on page 155).

Windows Users

If you have Windows clients, you should set up at least one share point to be used only by your Windows users. This provides a single point of access for the Windows users.

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 NFS service), could potentially expose your data to anyone on the Internet.

NFS share points don’t have the same level of security as AFP and SMB, which require user authentication (typing a user name and password) to gain access to a share point’s contents. If you have NFS clients, you may want to set up a share point to be used only by NFS users.

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 Settings:

- 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.
- 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 Settings.
- Don't export NFS volumes to World. Restrict NFS exports to a specific set of computers.

Setting Up Sharing

This section describes how to create share points and set access privileges for the share points. It also tells you how to configure the different protocols (AFP, SMB, FTP, and NFS) that you use to share items and how to automount share points on clients' desktops.

See "Managing Sharing" on page 215 for additional tasks that you might perform after you have set up sharing on your server.

Creating Share Points and Setting Privileges

You designate volumes, partitions, folders, or CDs to be share points using the Sharing module of Workgroup Manager.

To create a share point and set privileges:

- 1 In Workgroup Manager, click the Sharing button.
- 2 Select the volume or folder in the All list that you want to make a share point.
- 3 Click the Sharing tab.
- 4 Select "Share the selection and its contents."

Change the owner and group of the shared item by typing names into those fields or by dragging names from the Users & Groups drawer. You can open the drawer by clicking "Users & Groups."

Use the pop-up menus next to the fields to change the privileges for the Owner, Group, and 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.

Note: You should not assign Write Only access privileges to a file or share point. Only folders inside a share point should be assigned Write Only access privileges. Otherwise users won't be able to see the file or the contents of the share point.

Click the Copy button to apply the ownership and privileges to all items (files and folders) contained within the share point. This will override privileges that other users may have set.

By default, the new share point is shared through AFP, SMB, and FTP protocols. Use the Advanced pane to change the settings or stop sharing via these protocols or to export the item using NFS.

The Advanced settings are described in the following sections.

Configuring Apple File Protocol (AFP) Share Points

You can make share points available to Mac OS 8, Mac OS 9, and Mac OS X clients by sharing them using AFP.

To configure an AFP share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to share using AFP.
- 3 Click the Advanced tab and choose AFP Settings from the pop-up menu.
- 4 Select the “Share this item using Apple File Protocol” option.
- 5 Select “Allow AFP guest access” to allow clients to have guest access to this item.

For greater security, do not select this item.

- 6 Select “AFP clients see custom name for this item” if you want the share point to appear with a name different from its real one.
- 7 Enter the name you want AFP users to see in the text field.
- 8 Click Save.

Configuring Server Message Block (SMB) Share Points

You can make share points available to Windows clients by sharing them using Windows SMB.

To configure an SMB share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to share using SMB.
- 3 Click the Advanced tab and choose SMB Settings from the pop-up menu.
- 4 Select the “Share this item using Server Message Block” option.

- 5 Select “SMB clients see custom name for this item” if you want the item to appear with a name different from its real one.
- 6 Enter the name you want SMB users to see in the text field.
- 7 Click Save.

Configuring File Transfer Protocol (FTP) Share Points

You can make share points available to clients over the Internet by sharing them using FTP.

To configure an FTP share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to share using FTP.
- 3 Click the Advanced tab and choose FTP Settings from the pop-up menu.
- 4 Select the “Share this item using FTP” option.
- 5 Select “Allow FTP guest access” to allow FTP users with guest access to use this item.
For greater security, do not select this item.
- 6 Select “FTP clients see custom name for this item” if you want the item to appear with a name different from its real one.
- 7 Enter the name you want FTP users to see in the text field.
- 8 Click Save.

Sharing (Exporting) Items Using Network File System (NFS)

You can export share points to UNIX clients using NFS. (*Export* is the NFS term for sharing.)

To export an item using NFS:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to share using NFS.
- 3 Click the Advanced tab and choose NFS Export Settings from the pop-up menu.
- 4 Select “Export this item and its contents to” to export the item using NFS.
- 5 Use the pop-up menu to select who you want to be able to use this information—Client or World.

By default, 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.

For greater security, do not export to World.

- 6 Click Add to specify clients who can receive this export.

- 7 In the text box that appears, type the IP address or host name to add the client to the “Computer or Netgroup” list.
- 8 Select “Map Root user to nobody” if you want users identified as “root” on the remote client system to have only minimal privileges to read, write, and execute commands.
- 9 Select “Map All users to nobody” if you want all users to have minimal privileges to read, write, and execute.
- 10 Select “Read-only” 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 (a setting in the General tab), you can also define it as an NFS export to “World” with “Read only” privileges.

- 11 Click Save.

Automounting Share Points

Automount lets you have share points appear automatically on client computers when their computers start up or in their /Network/Servers folders. You can use the automount feature with AFP or NFS. When you configure a share point to mount automatically, a mount record is created in the Open Directory database.

You should publish automounts in the same shared domain in which the user records exist. This ensures that the users will always have access to the share point.

Be sure to enable guest access both for the share point and for the protocol under which it is shared.

Note: Automounted share points are available to clients only when their computers start up.

To automount a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to automount.
- 3 Click the Advanced tab and choose Automount Settings from the pop-up menu.
- 4 Select “Automount to client in domain.”
- 5 Use the pop-up menu to choose the shared directory domain to which you want to publish (automount) this item.

The share point will be mounted automatically on any computer configured to use the shared domain.

- 6 Enter your user name and password.
Note: You must be authorized (have write privileges) to change the domain.
- 7 After you are authenticated, click “Automount this item to clients in domain.”

- 8 For the Mount option:

Choose “dynamically in Network/Servers” if you want client users to see share points in the /Network/Servers folder of their computers. When a user selects a share point in the folder, the share point is mounted on the user’s computer. You should choose this option for home directories.

Choose “statically in” if you want the share point to mount automatically when the client computer starts up and enter the location in the user’s directory hierarchy where you want the item to appear. The share point appears as a folder in the location you specify.
- 9 For the “Mount using” option, choose whether you want to automount the share point using AFP or NFS.
- 10 Click Save.

Resharing NFS Mounts as AFP Share Points

Resharing NFS mounts (NFS volumes that have been exported to the Mac OS X Server) as AFP share points allows clients to access NFS volumes using the secure authentication of an AFP connection. Resharing NFS mounts also allows Mac OS 9 clients to access NFS file services on traditional UNIX networks.

To reshare an NFS mount as an AFP share point:

- 1 From the NFS server, export the directories you want to reshare to the Mac OS X server. Since AFP runs as root, the NFS export must map root-to-root so that AFP will be able to access the files for the clients. Restrict the export to the single AFP server (seen as the client to the NFS server). This can be made even more secure by having a private network for the AFP-to-NFS connection.
- 2 On the AFP server, create a mount record that mounts the reshared volumes in the /nfs-reshare directory.
- 3 Use the Sharing module in Workgroup Manager to share the NFS mounts as AFP share points. The NFS mounts appear as normal volumes in the All list. (You can also share the NFS mounts using SMB and FTP, but it is recommended that you only use AFP.) You can change privileges and ownership, but not enable quotas (quotas work only on local volumes). However, if quotas are enabled on the NFS server, they should apply to the reshared volume as well.

Managing Sharing

This section describes tasks you might perform after you have set up sharing on your server. Setup information appears in “Setting Up Sharing” on page 211.

Turning Sharing Off

Because sharing is not a service, you cannot turn sharing on and off on a Mac OS X Server. You “turn sharing off” by no longer sharing an item. You can also remove the share point or stop the file service that clients are using to access the share point.

To stop sharing an item:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the item you want to stop sharing.
- 3 Click the Advanced tab and choose the protocol used to share the item.
- 4 Deselect the “Share this item” option.

To completely stop sharing an item, repeat steps 3 and 4 for each protocol you used to share the item.

- 5 Click Save.

Removing a Share Point

To “remove a share point” is to stop sharing a volume or folder. You may want to notify users that you are removing a share point so that they know why the share point is no longer available.

To remove a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the share point you want to remove.
- 3 In the Sharing pane, deselect the “Share the selection and its contents” option.

Any Advanced and Automount settings that you have configured for the item are discarded.

Browsing Server Disks

You can view the folders (but not files) located on servers using the Sharing module of Workgroup Manager.

To browse the folders on a share point or server:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab to browse the folders of share items, or click the All tab to browse all the folders on the local server.

Viewing Share Points

Workgroup Manager lets you view all volumes and folders on a server or just the share points.

To view share points on a server:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab.

Copying Privileges to Enclosed Items

When you set the privileges for a share point, volume, or folder, you can copy the ownership and privileges to all the items contained on it.

To copy privileges:

- 1 In Workgroup Manager, click Sharing.
- 2 Select the item whose privileges you want to propagate.
To see shared items, select the Share Points tab. To see all volumes and folders on the server, select the All tab.
- 3 Click Copy.

Viewing Share Point Settings

You use Workgroup Manager to view the sharing and privilege settings for a share point.

To view sharing and privileges for a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Select the Share Points tab and select the share point you want to view.
- 3 Select the Sharing tab.

Changing Share Point Owner and Privilege Settings

You use the Workgroup Manager to view and change the owner and privileges for a share point.

To change privileges for a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Select the Share Points tab and select the share point you want to update.
- 3 Select the Sharing tab.

Change the owner and group of the shared item by typing names into those fields, or by dragging names from the Users & Groups drawer. You can open the drawer by clicking “Users & Groups.”

Use the pop-up menus next to the fields to change the privileges for the Owner, Group, and Everyone. *Everyone* is any user who can log in to the file server: registered users, guests, anonymous FTP users, and Web site visitors.

Changing the Protocols for a Share Point

You use the Advanced pane of Workgroup Manager to change the protocols for a share point.

To change the protocols for a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Select the share point you want to change.
Select the Share Points tab to see shared items.
- 3 Select the Advanced tab.
- 4 Use the pop-up menu to choose the protocol settings you want to change.
See the following sections for descriptions of the protocol settings:
 - “Configuring Apple File Protocol (AFP) Share Points” on page 212
 - “Configuring Server Message Block (SMB) Share Points” on page 212
 - “Configuring File Transfer Protocol (FTP) Share Points” on page 213
 - “Sharing (Exporting) Items Using Network File System (NFS)” on page 213

Deleting an NFS Client from a Share Point

You use the Advanced pane of Workgroup Manager to delete an NFS client from a share point.

To delete an NFS client from a share point:

- 1 In Workgroup Manager, click Sharing.
- 2 Click the Share Points tab and select the NFS share point you want to change.
- 3 Click the Advanced tab and choose NFS Export Settings from the pop-up menu.
- 4 Select an IP address from the list and click Remove.
- 5 Click Save.

Creating a Drop Box

A drop box is a shared folder that you set up to allow others to write to, but not read its contents.

Note: You should create drop boxes only within AFP share points. AFP is the only protocol that will automatically change the owner of an item put into a drop box to be the same as the owner of the drop box. For other protocols, the ownership of the item is not transferred even though the owner will no longer have access to the item.

To create a drop box:

- 1 If the folder you want to make into a drop box doesn't exist, create the folder within an AFP share point.

- 2 In Workgroup Manager, click Sharing.
- 3 Select Share Points and select the folder you want to use as a drop box.
- 4 Select the Sharing tab.
- 5 Set “Write Only” privileges for the users you want to have access to the drop box.

To create a drop box for a select group of users, enter the group name (or drag the group from the U&G Drawer) and choose “Write Only” privileges from the Group pop-up menu.

To create a drop box for all users, choose “Write Only” privileges from the Everyone pop-up menu. (For greater security, do not allow access to everyone—assign “None” for the Everyone privileges.)

- 6 Click Save.

Supporting Client Computers

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.

Solving Problems

Users Can't Access a CD-ROM Disc

- Make sure the CD-ROM disc is a share point.
- If you share multiple CDs, make sure each CD is shared using a unique name in the Sharing pane.

Users Can't Find a Shared Item

- If a user can't find a shared item, check the access privileges for the item. The user must have Read access privileges to the share point where the item is located and to each folder in the path to the item.
- Keep in mind that server administrators don't see share points the same way a user does over AFP 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.
- Although DNS is not required for file services, an incorrectly configured DNS could cause a file service to fail.

Users Can't See the Contents of a Share Point

- If you set Write Only access privileges to a share point, users won't be able to see its contents.

File Services

File services enable clients of the Mac OS X Server to access files, applications, and other resources over a network. Mac OS X Server includes four distinct 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.
- File Transfer Protocol (FTP) service lets you share files with anyone using FTP.
- Network File System (NFS) service lets you share files and folders with users who have NFS client software (UNIX users).

The following applications help you set up and manage file services:

- Server Settings—configure and turn file services on and off
- Workgroup Manager—share information and set access privileges
- Server Status—monitor the status of file services

Before You Begin

Before you start setting up file services you should determine which of the file services you need. In general, you will want to turn on and configure the file services needed to support all of your clients:

- Apple file service for Mac OS clients
- Windows services for Windows clients
- FTP service for clients using FTP to connect via the Internet
- NFS service for UNIX clients

You must configure and turn on file services in order for clients to be able to access shared information—the volumes and folders that you designate as share points—as described in Chapter 4, “Sharing.” You must also turn on Windows services if you want to share network printers using Windows Printing (SMB). Print service is described in Chapter 7, “Print Service,” on page 315.

For descriptions of the file services, see

- “Apple File Service” on page 224
- “Windows Services” on page 235
- “File Transfer Protocol (FTP) Service” on page 244
- “Network File System (NFS) Service” on page 256

Security Issues

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

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. See “Privileges” on page 205.

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 AFP or SMB Access settings, guest access is turned on for that service. For FTP, guest access is called “anonymous” access. Click the box to remove the checkmark and turn guest (or anonymous) access off.

AFP also allows you to control guest access for individual share points, if you allow guest access for the service. See “Configuring Apple File Protocol (AFP) Share Points” on page 212.

The equivalent to allowing guest access for NFS service is to export a shared item to World. Unlike guest access, which you set when configuring a service, exporting to World for NFS is an option you set when sharing an item. See “Sharing (Exporting) Items Using Network File System (NFS)” on page 213.

Note: NFS lacks authentication. NFS service allows users access to shared information based on their computers’ IP addresses. This is not as secure a method of preventing unauthorized access as the authentication techniques employed by the other file services that require users to enter their user names and passwords in order to gain access to shared information.

Client Computer Requirements

For information on client computer requirements, see “Supporting Client Computers” on page 259.

Setup Overview

Here’s is an overview of the basic steps for setting up file services.

Step 1: Read “Before You Begin”

Read “Before You Begin” on page 221 for issues you should consider before setting up file services.

Step 2: Define users

In order for users to be able access shared information, they must be given accounts that register them with the server. See Chapter 3, “Users and Groups,” for information about setting up user accounts.

Step 3: Create share points and set privileges

You share information on the network by designating volumes and folders as share points. Chapter 4, “Sharing,” tells you how to create share points and define access privileges for the shared information.

Step 4: Configure and start up file services

You use Server Settings to configure and start up file services. See these sections for setting up the individual services:

- “Setting Up Apple File Service” on page 225
- “Setting Up Windows Services” on page 237
- “Setting Up File Transfer Protocol (FTP) Service” on page 250
- “Setting Up NFS Service” on page 257

Step 5: Check client configurations

After you set up file services, you should make sure client computers are configured properly to connect to the server. Macintosh, Windows, and UNIX client computers all require TCP/IP in order to make connections to the server. See “Supporting Client Computers” on page 259.

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 3.1, which supports new features such as Unicode file names and 64-bit file sizes. *Unicode* is a standard that assigns a unique number to every character regardless of language or the operating system used to display the language.

One difference in the new Apple file service is that AppleTalk is no longer supported as a connection method. Mac OS X Server advertises its services over AppleTalk so clients using AppleTalk can see servers in the Chooser, but they will need to connect to the server using TCP/IP. See "Supporting Mac OS X Clients" on page 259 and "Supporting Mac OS 8 and Mac OS 9 Clients" on page 260.

Automatic Reconnect

Mac OS X Server provides the ability to automatically reconnect Mac OS X clients that have become idle or gone to sleep. When clients become idle or go to sleep, the Mac OS X Server disconnects those clients to free up server resources. Mac OS X Server can save Mac OS X client sessions, however, allowing these clients to resume work on open files without loss of data. You configure this setting in the Idle Users pane of the Apple file service configuration window. See "Configuring Apple File Service Idle Users Settings" on page 228.

Find By Content

Mac OS X clients can use Sherlock to search the contents of AFP servers. This feature enforces privileges so that only files to which the user has access are searched.

Kerberos Authentication

Apple File Service supports Kerberos authentication. *Kerberos* is network authentication protocol developed at MIT to provide secure authentication and communication over open networks. In addition to the standard authentication method, Mac OS X Server utilizes Generic Security Services Application Programming Interface (GSSAPI) authentication protocol to support Kerberos v.5. You specify the authentication method using the Access pane of Configure Apple File Service. See "Configuring Apple File Service Access Settings" on page 226. For information about integrating your Mac OS X Server with Kerberos, see "Understanding Kerberos" on page 198.

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

Before You Set Up Apple File Service

If you asked the Server 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. The following section steps you through each of the Apple file service settings.

Setting Up Apple File Service

You set up Apple file service by configuring four groups of settings in the Configure Apple File Service window:

- **General**—set information that identifies your server, enable automatic startup, and create a login message for Apple file service
- **Access**—set up client connections and guest access
- **Logging**—configure and manage logs for Apple file service
- **Idle Users**—configure and administer idle user settings

The following sections describe the tasks for configuring these settings. A fifth section tells you how to start up Apple file service after you have completed its configuration.

Configuring Apple File Service General Settings

You use the General pane to set identifying information about your server, enable automatic startup, and create a login message for Apple file service.

To configure Apple file service General settings:

- 1** In Server Settings, click the File & Print tab.
- 2** Click Apple and choose Configure Apple File Service.
- 3** Click the General tab.
- 4** In the Computer Name field, type the name for the server 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.

- 5** Select "Start Apple File Service on system startup" to ensure that file services will be available if the server is restarted after a power failure or other unexpected event.

This option is selected automatically when you start the server and in most cases it's best to leave it selected.

- 6 Select "Enable browsing with Network Service Location" 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 also registers with Rendezvous and 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 16, "SLP DA Service," for more information about Service Location Protocol (SLP) and IP multicasting.

- 7 Select "Enable browsing with AppleTalk" if you want Mac OS 8 and Mac OS 9 clients 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. Clients will be able to see the server in the Chooser, but will need to connect using TCP/IP.

- 8 Choose a character set in the "Encoding for older clients" pop-up menu for the server that matches the character set used by your Mac OS 8 and Mac OS 9 client users.

When Mac OS 9 and earlier clients are connected, the server converts file names from the system's UTF-8 to the chosen set. This has no effect on Mac OS X client users.

- 9 Select "Do not send same message twice to the same user" if you want users to see your greeting only the first time they log in to the server.

If you change the message, users will see the new message the next time they connect to the server.

- 10 In the Logon Greeting field, type the message that you want users to see when they connect.
Note: The logon message does not appear when a user logs into his or her home directory.
- 11 Click Save.

Configuring Apple File Service Access Settings

You use the Access pane to control client connections and guest access.

To configure Apple file service access settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Access tab.
- 4 Choose the authentication method you want to use: Standard, Kerberos, or Any Method.
- 5 Select "Enable Guest access" 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 in share points that allow guest access. For better security, do not select this option.

Note: If you allow guest access for Apple file service, AFP lets you control guest access for individual share points.

See “Configuring Apple File Protocol (AFP) Share Points” on page 212.

- 6 Select “Enable secure connections” if you want to allow clients to connect using secure AFP (uses SSH).

- 7 Under the “Maximum client connections (including Guests)” option:

Select Unlimited if you don’t want to limit the number of users who can be connected to your server at one time.

Enter a number if you want to limit the number of simultaneous users.

The maximum number of simultaneous users is also limited by the type of license you have. For example, if you have a 10-user license, then a maximum of 10 users can connect at one time.

Limiting the number of connections can free resources to be used by other services and applications.

- 8 Under the “Maximum Guest connections” option:

Select Unlimited if you don’t want to limit the number of guest users who can be connected to your server at one time.

Enter a number if you want to limit how many of your maximum client connections can be used by guests. This number cannot be greater than the number of client connections allowed.

- 9 Click Save.

Configuring Apple File Service Logging Settings

You use the Logging pane to configure and manage logs for Apple file service.

To configure Apple file service logging settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Logging tab.
- 4 Select “Enable Access log” if you want to create an access log.
The access log stores information about any of the events you select.
- 5 Select “Archive every ___ days” and type the number of days to specify how often the log file contents are saved to an archive.

The server closes the log at the end of each archive period, renames the log to include the current date, and 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 7 days.

- 6 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.

Consider your server's disk size when choosing events to log. The more events you choose, the larger the log file.

- 7 Select "Error Log: Archive every ___ days" and type the number of days to specify how often the error log file contents are saved to an archive.

The server closes the log at the end of each archive period, renames the log to include the current date, and 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 7 days.

- 8 Click Save.

You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See "Log Rolling Scripts" on page 555.

Configuring Apple File Service 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 configure Apple file service Idle Users settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Idle Users tab.
- 4 Select "Allow clients to sleep ___ hour(s)—will not show as idle" and type the number of hours to allow clients to automatically reconnect to the server after becoming idle or going to sleep.

Although the server disconnects clients when they become idle or go to sleep, the clients' sessions are maintained for the specified period. When a user resumes work within that time, the client is reconnected with no apparent interruption. If a longer period elapses, open files are closed and any unsaved work is lost.

- 5 Select "Disconnect idle users after ___ minutes" and type the number of minutes to disconnect idle users after the specified time.

This ensures that server resources are available to active users.

Mac OS X version 10.2 (and later) clients will be able to resume work on open files within the limits of the “Save sleep and reconnect session” setting.

- 6 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, or Idle users who have open files.

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

- 7 Type the message in the “Disconnect Message” field that 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. For example, Mac OS X version 10.2 (and later) clients will not see this message since they can automatically reconnect to the server.

- 8 Click Save.

Starting Apple File Service

Start Apple file service to make the service available to your client users.

To start Apple file service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Start Apple File Service.

A globe appears on the service icon when the service is turned on.

You can also set Apple file service to start up automatically each time your server starts up. See “Starting Up Apple File Service Automatically” on page 231.

Managing Apple File Service

This section tells you how to perform day-to-day management tasks for Apple file service once you have it up and running.

Viewing Apple File Service Status

You use Server Status to check the status of all Mac OS X Server devices and services.

To view Apple file service status:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select AppleFile in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Overview tab to see whether the service is running and when it started, its throughput and number of connections, and whether guest access and logging are enabled.
- 3 Click the Logs tab to see the access and error logs.
Use the Show pop-up menu to choose which log to view.
- 4 Click the Connections tab to see a list of the users currently connected to Apple file service.
The table includes the user name, type of connection, user's IP address or domain name, duration of connection, and the time since the last data transfer (idle time).
Buttons at the bottom of the pane let you send a message to a user and disconnect the user.
- 5 Click the Graphs tab to see graphs of connected users or throughput.
Use the pop-up menu to choose which graph to view. Adjust the time scale using the slider at the bottom of the pane.

Viewing Apple File Service Logs

You use Server Status to view the error and access logs for Apple file service (if you have enabled them). You can also save selected log entries in another file or folder.

To view logs:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select AppleFile in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Logs tab and use the Show pop-up menu to choose between the access and error logs.

Stopping Apple File Service

Important When you stop Apple file service, connected users may lose any information they have not saved.

To stop Apple file service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Stop Apple File Service.
- 3 Enter the length of time you want to wait before file service stops.
- 4 Type a message in the Additional Message field if you want to send a message to users in addition to the default message when the service is stopped.

- 5 Click Shutdown.

Note: Stopping the server disables the “Start Apple File Service on system startup” option.

Starting Up Apple File Service Automatically

You can set Apple file service to start up automatically each time your server starts up.

Note: Apple file service must already be running before you can set this option. See “Starting Apple File Service” on page 229.

To set Apple file service to start up automatically:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the General tab.
- 4 Select “Start Apple File Service on system startup” and click Save.

Changing the Apple File Server Name

By default, Apple file service registers itself on the network using its IP address, and the server’s DNS name is the name users see when using the Chooser or the Network Browser.

To change the name of the file server:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the General tab.
- 4 Type a new name for your server in the Computer Name field and click Save.

The name you enter here must be unique among all computers connected to the network.

Registering With Network Service Locator

You can register your Apple file server with Network Service Locator (NSL) to allow users to find the server by browsing through available servers. Otherwise, users must type the server’s host name or IP address.

To register with NSL:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the General tab, select “Register with Network Service Location,” and click Save.

This option also registers with Rendezvous.

If you turn on this option, you must also enable and configure Service Location Protocol (SLP) service on your network router. See Chapter 16, “SLP DA Service,” for more information about SLP.

Enabling AppleTalk Browsing for Apple File Service

If you enable browsing with AppleTalk, users can see your servers and other network resources using the Chooser.

To enable browsing via AppleTalk:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Access tab and select “Allow clients to browse using AppleTalk.”
- 4 Click Save.

Setting Maximum Connections for Apple File Service

If your server provides a number of services, you can improve server performance by limiting the number of clients and guests who can be connected at the same time.

To set the maximum number of connections:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Access tab.
- 4 Under the “Maximum client connections (including Guests)” option type the maximum number of connections you want to allow.
- 5 Click Save.

Turning On Access Logs for Apple File Service

The access log can record any time a user logs in or out, opens a file, creates a file or folder, or deletes a file or folder.

To turn on access logs:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Logging tab and select “Enable access log.”
- 4 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.

Consider your server’s disk size when choosing events to log. The more events you choose, the larger the log file.

You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See “Log Rolling Scripts” on page 555.

Archiving Apple File Service Logs

You can specify how often the contents of the access and error logs for Apple file service are saved to an archive file.

To set how often logs are archived:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Logging tab.
- 4 Make sure the “Enable Access log” option is selected.
- 5 Select “Archive every ___ days” and type the number of days to specify how often the log file contents are saved to an archive.

The server closes the log at the end of each archive period, renames the log to include the current date, and 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 7 days.

- 6 Select “Error Log: Archive every ___ days” and type the number of days to specify how often the error log file contents are saved to an archive.

The server closes the log at the end of each archive period, renames the log to include the current date, and 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 7 days.

- 7 Click Save.

You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See “Log Rolling Scripts” on page 555.

Disconnecting a User From the Apple File Server

To disconnect a user:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Show Apple File Service Status.
- 3 Select the user and click Disconnect.
- 4 Enter the amount of time before the user is disconnected, and type a disconnect message. If you don't type a message, a default message will appear.
- 5 Click Disconnect.

Disconnecting Idle Users From the Apple File Server

You can set Apple file service to automatically disconnect users who are connected to the server but have not used the server volume for a period of time.

To set how the server handles idle users:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Idle Users tab and choose the settings you want to use.
- 4 In the Disconnect Message field, type the message you want client users to see when they are disconnected.

If you don't enter a message, a default message will appear.

- 5 Click Save.

Allowing Guest Access to the Apple File Server

Guests are users who can see information on your server without using a name or password to log in. For better security, do not allow guest access.

To enable guest access:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the Access tab and select "Allow Guest access."
- 4 Under the "Maximum guest connections" option:

Select Unlimited if you don't want to limit the number of guest users who can be connected to your server at one time.

Enter a number if you want to limit how many of your maximum client connections can be used by guests

- 5 Click Save.

Creating a Login Greeting for Apple File Service

The login greeting is a message users see when they log in the server.

To create a login greeting:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Apple and choose Configure Apple File Service.
- 3 Click the General tab and type your message in the Logon Greeting field.
- 4 Select "Do not send same message twice to the same user" if you want users to see your greeting only the first time they log in to the server.

If you change the message, users will see the new message the next time they connect to the server.

- 5 Click Save.

Sending a Message to an Apple File Service User

You use the Connections pane of Server Status to send messages to clients using Apple file service.

To send a user a message:

- 1 In Server Status, locate the name of the server in the Devices & Services list to which the user is connected and select AppleFile in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click Connections and select the user's name in the list.
- 3 Click Send Message.
- 4 Type the message you want to send and click Send.

Windows Services

Windows services in Mac OS X Server provide four native services to Windows clients. These services are

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

Windows services use the Windows code page setting to display the correct language for the client.

Samba is public-domain software that provides file and print services to Windows clients. For more information about Samba, refer to the Samba web site:

www.samba.org

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

Before You Set Up Windows Services

If you plan to provide Windows services on your Mac OS X Server, read the following sections for issues 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. Although Mac OS X Server does not require any special software or configuration on Windows client computers, you may want to read “Supporting Windows Clients” on page 261.

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. See “Creating Share Points and Setting Privileges” on page 211.

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 Windows file names to 31 characters (the limit for Mac OS 8 and Mac OS 9 clients).
- Don't use symbols or characters with accents in the names of shared items.

Windows User Password Validation

Mac OS X Server supports several methods of validating Windows user passwords. Password Server is the recommended method. It supports LDAP as well as NetInfo because the directory does not store the password, just a pointer to the proper Password Server and user ID. The Password Server database is a root readable file, and the contents are encrypted. Passwords are not accessible over the network for reading—they can only be verified. See “Using a Password Server” on page 195 and “Setting Up an Open Directory Domain and Password Server” on page 92.

Authentication Manager is supported for upgrades from earlier versions of Mac OS X Server (10.1 and earlier). Existing users will continue to use Authentication Manager. (If you export from Mac OS X Server and reimport, you do not get the `tim_password` set. You must manually set the password for each user after import.) You can enable Authentication Manager from the command line. Use Basic password validation. You should set Authentication Manager passwords on the server which is hosting the domain you are editing. See *Understanding and Using NetInfo* for information on how to use the command line utilities for Authentication Manager. This document is available on the Mac OS X Server Web site:

www.apple.com/macosx/server/

Note: Authentication Manager is only supported with NetInfo.

Setting Up Windows Services

You set up Windows services by configuring four groups of settings:

- General—set information that identifies your Windows server and enable automatic startup
- Access—allow guest access and set the maximum number of client connections
- Logging—choose the level of detail you want in your log
- Idle Users—set up name resolution and enable browsing across subnets

Because the default settings will work well in most cases, it may be that all you need to do to set up Windows services is to start it. Nonetheless, you should take a look at the settings and change anything that isn't appropriate for your network. Each of the settings is described in the following sections on configuration. After the configuration tasks, other topics tell you how to start up Windows services.

Configuring Windows Services General Settings

You use the General pane to set identifying information about your Windows server and to enable automatic startup.

To configure Windows General settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the General tab.
- 4 In the Server Name field, 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.”

- 5 In the Workgroup field, 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.

- 6 In the Description field, type a description that is meaningful to you or your users.

This description appears in the Network Neighborhood window on client computers, and it is optional.

The Description cannot exceed 48 characters.

- 7 Use the Code Page pop-up menu to choose the code page for the language client computers will use.

- 8 Select the “Start Windows Services on system startup” option if you want to ensure that the server is restarted after a power failure or other unexpected event.

This option is automatically selected when you start the server and in most cases it’s best to leave it selected.

Configuring Windows Services Access Settings

You use the Access pane to allow guest access and set the maximum client connections.

To configure Windows services Access settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Access tab.
- 4 Select “Allow Guest access” 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.

For better security, do not select this option.

- 5 Below “Maximum client connections” choose Unlimited if you do not want to limit the number of users who can be connected to your server at one time.
- 6 If you want to limit the number of simultaneous users, click the button below Unlimited and enter the number of connections.

The maximum number of simultaneous users is also limited by the type of license you have. For example, if you have a 10-user license, then a maximum of 10 users can connect at one time.

Limiting the number of connections can free resources to be used by other services and applications.

Configuring Windows Services Logging Settings

You use the Logging pane to choose the level of detail you want in your logs.

To configure Windows services Logging settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Logging tab.
- 4 Use the Detail Level pop-up menu to choose the level of detail you want logged: None, Minimal, or Verbose.

The more detailed the logging, the larger the log file.

The table below shows the level of detail you 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

You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See “Log Rolling Scripts” on page 555.

Configuring Windows Services Neighborhood Settings

You use the Neighborhood pane to set up name resolution and enable browsing across subnets.

To configure Windows services Neighborhood settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.

- 3 Click the Neighborhood tab.
- 4 Under WINS Registration, choose whether you want to register with a WINS server, either locally or externally:

Choose “Off” to prevent your server from registering itself with any external WINS server or local name resolution server.

Choose “Enable WINS server” to have the file server provide local name resolution services. This allows clients across multiple subnets to perform name/address resolution.

Choose “Register with WINS server” 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.
- 5 Under Workgroup/Domain Services, choose whether to enable domain browsing services:

“Master Browser” provides browsing and discovery of servers in a single subnet.

“Domain Master Browser” provides browsing and discovery of servers across subnets.

Starting Windows Services

Start Windows services to make the services available to your client users.

To start Windows services:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Start Windows Service.

A globe appears on the service icon when the service is turned on.

Managing Windows Services

This section tells you how to perform day-to-day management tasks for Windows services once you have the services up and running.

Stopping Windows Services

Important When you stop Windows services, connected users will lose any information they haven’t saved.

To stop Windows services:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Stop Windows Services.

Setting Automatic Startup for Windows Services

You can set Windows services to start automatically each time your server starts up.

To set automatic startup:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the General tab, then click “Start Windows Services on system startup.”
- 4 Click Save.

Changing the Windows Server Name

The default server 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.

To change the file server name:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the General tab and enter a name in the Server Name field.
- 4 Click Save.

Finding the Server’s Workgroup Name

You can discover the server’s workgroup name in the General pane of Configure Windows Services.

To find the server’s workgroup name:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.

The Workgroup name is shown in the General pane.

Checking Windows Services Status

You use Server Status to check the status of all Mac OS X Server devices and services.

To view Windows services status:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select Windows in the list of services under the server name.

If the services aren’t visible, click the arrow to the left of the server name.

- 2 Click the Overview tab to see whether the services are running and when they started, the number of connections, and whether guest access and logging are enabled.
- 3 Click the Logs tab to see the Windows file service and name service logs.

Use the Show pop-up menu to choose which log to view.

- 4 Click the Connections tab to see a list of the users currently connected to the Windows services.

The list includes the users' names, IP addresses, and duration of connections. A button at the bottom of the pane lets you disconnect a user.

- 5 Click the Graphs tab to see graphs of connected users or throughput.

The connected users are shown as a column chart. Use the slider to adjust the time scale.

Registering with a WINS Server

Windows Internet Naming Service (WINS) matches server names with IP addresses. You can use your server as the local name resolution server, or you can register with an external WINS server.

To register your server with a WINS server:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Neighborhood tab and select one of the options under WINS Registration.
If you select "Register with WINS server," enter the IP address or DNS name of the external WINS server you want to use.
- 4 Click Save.

Enabling Domain Browsing for Windows Services

If there are no Microsoft servers on your subnet or network to control domain browsing, use these options to restrict domain browsing to a single subnet or allow browsing across your network.

To enable domain browsing:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Neighborhood tab, then select Master Browser or Domain Master Browser.
Select Master Browser to let clients browse for and locate servers in a single subnet.
Select Domain Master Browser to let clients browse for and locate servers across your network (subnets).
- 4 Click Save.

Setting Maximum Connections for Windows Services

You can limit the potential resources consumed by Windows services by limiting the maximum number of connections.

To set the maximum number of connections:

- 1 In Server Settings, click the File & Print tab.

- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Access tab.
- 4 Click Unlimited, or type the maximum number of connections you want to allow.
- 5 Click Save.

Setting Up the Windows Services Log

When you set up logging for Windows services, you can choose the level of detail you want to log.

To set up a log for Windows services:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Logging tab, then use the Detail Level pop-up menu to choose the level of detail you want to log: None, Minimal, or Verbose.

The more detailed the logging, the larger the log file.

- 4 Click Save.

Disconnecting a User From the Windows Server

Important Users who are disconnected will lose any information they haven't saved.

To disconnect a user:

- 1 In Server Status, locate the name of the server the user is connected to in the Devices & Services list.
- 2 Select Windows in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 3 Click the Connections tab and select the user you want to disconnect.
- 4 Click the Disconnect button.

Allowing Guest Access in Windows Services

Guests are users who can see information on your server without using a name or password to log in. For better security, do not allow guest access.

To enable guest access to the server:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the Access tab and select "Allow Guest access."
- 4 Click Save.

Assigning the Windows Server to a Workgroup

Users see the workgroup name 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 name.

To assign a workgroup name:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Windows and choose Configure Windows Services.
- 3 Click the General tab and type a name in the Workgroup field.
- 4 Click Save.

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.

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 the following sections.

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 directories and data 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 expands the restricted environment to allow access to symbolic links and aliases while still providing a secure FTP environment. FTP users can potentially access directories and their contents located anywhere on the server, as long as the directories are share points configured for FTP. Access to the FTP root and FTP share points for individual users is determined by the user environment you specify (as described in the following section) and the access privileges set for the users. For information about creating share points and setting access privileges, see Chapter 4, "Sharing." See "Configuring the FTP User Environment" on page 254.

User Environments

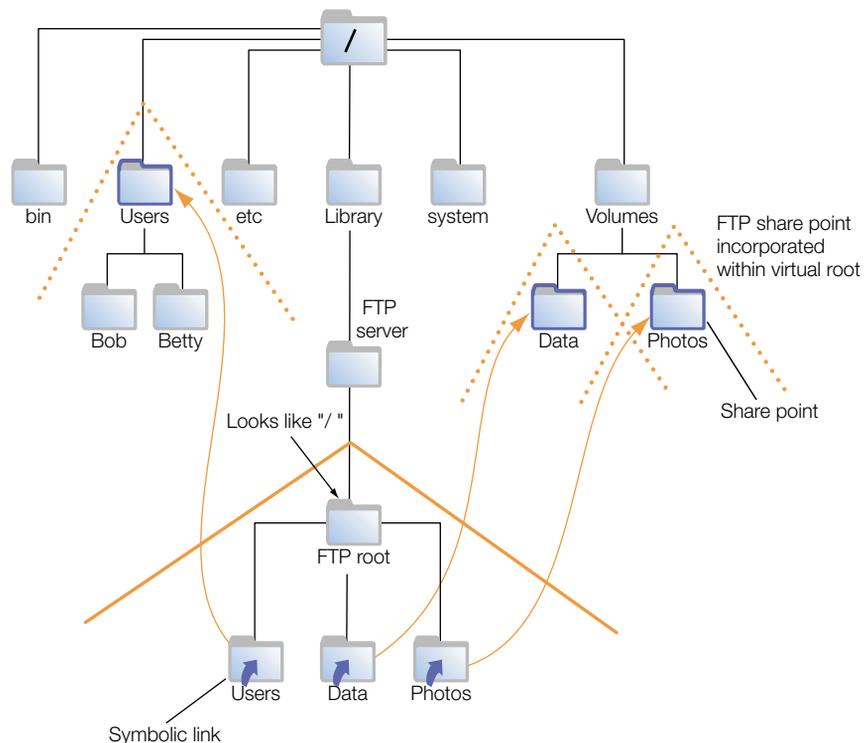
Mac OS X Server provides three different user environments that determine how the FTP root, share points, and home directories are made available to FTP users:

- FTP root and share points
- Home directory and FTP root
- Home directory only

You specify the user environment in the Advanced pane of Configure FTP Service. See “Configuring FTP Advanced Settings” on page 252.

FTP Root and Share Points

The “FTP Root and Share Points” user environment gives access—for both real and anonymous users—to the FTP root and any FTP share points to which the users have access privileges, as shown in the following figure.



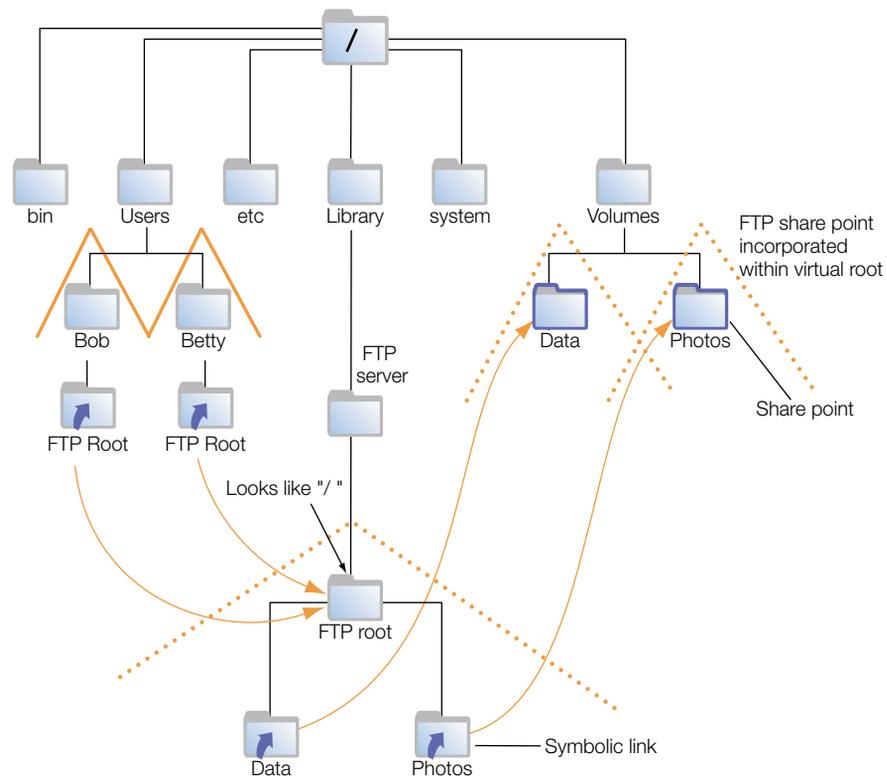
Users access FTP share points through symbolic links attached to the FTP Root directory. The symbolic links are created automatically when you create the FTP share points.

Note that in this example, `/Users`, `/Volumes/Data`, and `/Volumes/Photos` are FTP share points. All users can see the home directories of other users because they are subdirectories of the Users share point.

Important Regardless of the user environment setting, anonymous users and users without home directories are always logged into the “FTP Root and Share Points” environment.

Home Directory and FTP Root

When the user environment option is set to “Home Directory and FTP Root,” real users are logged into their home directories and have access to the FTP root by means of a symbolic link automatically created in their home directories. Other FTP share points are accessible through symbolic links in the FTP root. As always, access to the FTP share points is controlled by the access privileges they are assigned.

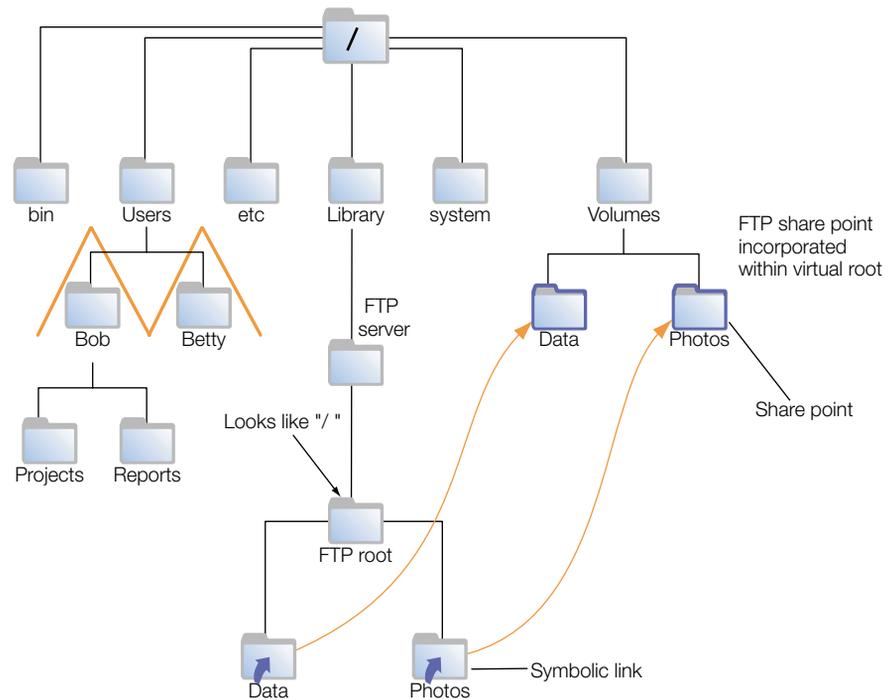


In this scenario, the `/Users` folder is not an FTP share point and users are not able to see the home directories of other users.

If you create a custom FTP root, then the symbolic link in users' home directories will reflect that custom name. For example, if you set a custom FTP root directory to be `/Volumes/Extra/NewRoot`, the symbolic link created in the user's home directory would be called `NewRoot`.

Home Directory Only

In the Restricted user environment, real users are confined to their home directories and do not have access to the FTP root or other FTP share points, as shown in the following illustration.



Anonymous users and users without home directories still have access to the FTP root and FTP share points. So that these users cannot see the home directories of real users, the /Users folder is not set up as an FTP share point.

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 file-name 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 the files 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
.gz	DEFLATE compression
.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
.dmg	Mac OS X disk image

Custom FTP Root

For increased security, Mac OS X Server lets you create a custom FTP root. You specify the directory path of the custom FTP root using the Advanced pane of Configure FTP Service. See “Configuring FTP Advanced Settings” on page 252. The custom root takes the place of the default FTP root directory.

Kerberos Authentication

FTP supports Kerberos authentication. You specify the authentication method using the Advanced pane of Configure FTP Service. See “Configuring FTP Advanced Settings” on page 252. For information about Kerberos, see “Kerberos Authentication” on page 224.

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

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 special directory named “uploads” in the FTP root. 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

Setup Overview

Here is an overview of the major steps for setting up FTP service.

Step 1: Before You Begin

Read “Before You Set Up FTP Service” on page 248 for issues you should keep in mind when you set up FTP service.

Step 2: Configure FTP General settings

The General settings let you display banner and welcome messages, set the number of login attempts, and provide an administrator email address. See “Configuring FTP General Settings” on page 250.

Step 3: Configure FTP Access settings

The Access Settings let you specify the number of real and anonymous users. See “Configuring FTP Access Settings” on page 251.

Step 4: Configure FTP Logging settings

The Logging settings let you specify the events you want to log for real and anonymous users. See “Configuring FTP Logging Settings” on page 251.

Step 5: Configure FTP Advanced settings

The Advanced settings specify a custom FTP root to use. See “Configuring FTP Advanced Settings” on page 252.

Step 6: Create an “uploads” folder for FTP users (optional)

If you enabled anonymous access in Step 2, you may want to create a folder for anonymous users to upload files. The folder must be named “uploads.” It is not a share point, but must have appropriate access privileges. See “Creating an Uploads Folder for Anonymous Users” on page 253.

Step 7: Create share points and share them using FTP

Use the Sharing module of Workgroup Manager to specify the share points that you want to make available through FTP. You must explicitly configure a share point to use FTP in order for FTP users to be able to access the share point. See “Creating Share Points and Setting Privileges” on page 211 and “Configuring File Transfer Protocol (FTP) Share Points” on page 213.

Step 8: Start FTP service

After you have configured FTP, start the service to make it available. See “Starting FTP Service” on page 252.

Setting Up File Transfer Protocol (FTP) Service

Configuring FTP General Settings

The General settings let you display banner and welcome messages, set the number of login attempts, and provide an administrator email address.

To configure the FTP General settings:

- 1** In Server Settings, click the File & Print tab.
- 2** Click FTP and choose Configure FTP Service.
- 3** Click the General tab.
- 4** Select the “Show Banner Message” option to display a message to users before they log in to the server.
- 5** Click the Edit Banner button to create or revise a banner message.
- 6** Select the “Show Welcome Message” option to display a message to users after they have logged in to the server.
- 7** Click the Edit Welcome button to create or revise a welcome message in the window that appears.
- 8** Select the “Disconnect after ___ failed login attempts” and type a number to limit the number of failed login attempts users can make before they are automatically disconnected from the server.

- 9 In the “Administrator E-mail Address” field, enter an email address if you want to provide a way for users to contact the administrator.
- 10 Click Save.

Configuring FTP Access Settings

The Access Settings let you specify the number of real and anonymous users.

To configure the FTP Access settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Access tab.
- 4 Enter a value in the “Allow a maximum of ___ real users” 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 Workgroup Manager.

- 5 Select “Enable anonymous access” to allow anonymous users to connect to the server and transfer files.

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 addresses.

Before selecting this option, 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.”

- 6 Enter a value in the “Allow a maximum of ___ anonymous users” field to set the maximum number of anonymous users who can connect to your server at the same time.
- 7 Click Save.

Configuring FTP Logging Settings

The Logging settings let you specify the events you want to log for real and anonymous users.

To configure the FTP Logging settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Logging tab.
- 4 In the “Log Real Users” section, select the events you want to appear in the FTP log for real users.

You can select FTP Commands, Rule Violation Attempts, Uploads, and Downloads.

- 5 In the “Log Anonymous Users” section, select the events you want to appear in the FTP log for anonymous users.

You can select FTP Commands, Rule Violation Attempts, Uploads, and Downloads.

- 6 Click Save.

Configuring FTP Advanced Settings

The Advanced settings allow you to specify a custom FTP root. A custom FTP root creates a higher level of security by isolating the files accessible through FTP from the main directory of the server.

To configure the FTP Advanced settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Advanced tab.
- 4 Select the “Use custom FTP root” and enter the pathname in the Path field if you want to create a custom FTP root.

See “Custom FTP Root” on page 248.

- 5 Choose the type of authentication you want to use: Standard, Kerberos, or Any Method.
- 6 Choose the type of user (chroot) environment you want to use: FTP Root and Share Points, Home Directory and FTP Root, or Home Directory Only.

See “User Environments” on page 245.

Starting FTP Service

Start FTP file service to make the service available to your client users.

To start FTP service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Start FTP Service.

A globe appears on the service icon when the service is turned on.

Managing File Transfer Protocol (FTP) Service

This section tells you how to perform day-to-day management tasks for FTP service once you have it up and running.

Stopping FTP Service

Important When you stop FTP service, connected users will be disconnected without warning.

To stop FTP service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Stop FTP.

Setting Up Anonymous FTP Service

You can allow guests to log in to your FTP server with the user name “ftp” or “anonymous.” They do not need a password to log in, but they will be prompted to enter their email addresses.

For better security, do not enable anonymous access.

To set up anonymous FTP service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP.
- 3 Click the Access tab.
- 4 Select “Anonymous access enabled.”
- 5 Click Save.

If the “Anonymous access enabled” box has a checkmark, anonymous access is already enabled.

Creating an Uploads Folder for Anonymous Users

The uploads folder provides a place for anonymous users to upload files to the FTP server. It must exist at the top level of the FTP root directory and be named “uploads.” (If you have set up a custom FTP root directory, then the uploads folder must be at the root of that directory.) Use the Finder to create the folder and set write privileges for guest users.

Specifying a Custom FTP Root

The Advanced settings allow you to specify the path for a custom FTP root.

To specify a custom FTP root:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Advanced tab.
- 4 Enter the pathname for the FTP root.
- 5 Select the “Use custom FTP root” and enter the pathname in the Path field if you want to create a custom FTP root.
- 6 If it does not already exist, create the directory you’ve specified and configure it as an FTP share point.

Specifying the FTP Authentication Method

You use the Advanced pane of Configure FTP Service to specify the authentication method.

To specify the FTP authentication method:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Advanced tab.
- 4 Choose the type of authentication you want to use: Standard, Kerberos, or Any Method. See “Kerberos Authentication” on page 248.

Configuring the FTP User Environment

You use the Advanced pane of Configure FTP Service to specify the user environment.

To configure the FTP user environment:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Advanced tab.
- 4 Choose the type of user environment you want to provide.

The “FTP Root and Share Points” environment sets up the Users directory as a share point. Real users log in to their home directories, if they are available within the restricted environment. Both real and anonymous users can see other users’ home directories in a share point. (The directories are only accessible to users who have access privileges, however.)

The “Home Directory and FTP Root” environment logs real FTP users in to their home directories. They have access to their home directories, to the FTP root, and to FTP share points.

The “Home Directory Only” environment restricts real FTP to users’ home directories only.

Regardless of the user environment you choose, access to all data is controlled by access privileges.

Anonymous users and real users who don’t have home directories (or whose home directories are not located in a share point to which they have access) are always logged in at the root level of the restricted FTP environment.

Viewing FTP Logs

You use Server Settings to view FTP logs.

To view FTP logs:

- 1 In Server Settings, click the File & Print tab.

- 2 Click FTP and choose Configure FTP Service.
- 3 Click the Logging tab.
- 4 Select the log options for real users: FTP Commands, Rule Violation Attempts, Uploads, and Downloads.
- 5 Select the log options for anonymous users: FTP Commands, Rule Violation Attempts, Uploads, and Downloads.

Displaying Banner and Welcome 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.

To display banner and welcome messages to users:

- 1 In Server Settings, click the File & Print tab.
- 2 Click FTP and choose Configure FTP Service.
- 3 Click the General tab.
- 4 Select the “Show Banner Message” option to display a message to users before they log in to the server.
- 5 Click the Edit Banner button to create or revise a banner message.
- 6 Select the “Show Welcome Message” option to display a message to users after they have logged in to the server.
- 7 Click the Edit Welcome button to create or revise a welcome message in the window that appears.
- 8 Click Save.

Displaying Messages Using message.txt files

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.

Using 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.

Network File System (NFS) Service

Network File System is the protocol used for file services on UNIX computers. Use NFS to provide file service for your UNIX clients (other than Mac OS X clients). You can export a shared item to a set of client computers or to “World.” Exporting an NFS volume to World means that anyone who can access your server can also access that volume.

Note: The NFS term for sharing is *export*. This guide, therefore, uses that term to be consistent with standard NFS terminology.

You use the NFS module of Server Settings to configure and manage NFS service. You also use the Sharing module of Workgroup Manager to set privileges and access levels for the share points or folders you want to export.

Before You Set Up NFS Service

Be sure to consider the security implications of exporting in NFS before you set up NFS service.

Security Implications

NFS was created for a secure networking environment, in which you can trust the client computer users and the people who administer the clients. Whereas access to Apple file service, Windows file sharing, and FTP service share points is controlled by authentication (user name and password), access to NFS shared items is controlled by the client software and file permissions.

NFS 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 the computer. 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.

With NFS, it’s possible for a user to *spoof* 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. If you have Internet access and plan to export to World, your server should be behind a firewall.

Setup Overview

Here is an overview of the major steps for setting up NFS service.

Step 1: Before You Begin

Read “Before You Set Up NFS Service” on page 256 for issues you should keep in mind when you set up NFS service.

Step 2: Configure NFS settings

The NFS settings let you set the maximum number of daemons and choose how you want to serve clients—via TCP, UDP, or both. See “Configuring NFS Settings” on page 257.

Step 3: Create share points and share them using NFS

Use the Sharing module of Workgroup Manager to specify the share points that you want to export (share) using NFS. You must explicitly configure a share point to use NFS in order for NFS users to be able to access the share point. See “Creating Share Points and Setting Privileges” on page 211, “Sharing (Exporting) Items Using Network File System (NFS)” on page 213, and “Automounting Share Points” on page 214.

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 Settings.

Setting Up NFS Service

Configuring NFS Settings

The NFS settings let you set the maximum number of daemons and choose how you want to serve clients—via TCP, UDP, or both.

To configure NFS settings:

- 1 In Server Settings, click the File & Print tab.
- 2 Click NFS and choose Configure NFS.
- 3 Enter a value in the “Allow a maximum of ___ daemons” field to set 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 requests from clients. The more daemons that are available, the more concurrent clients can be served. Typically, four to six daemons is adequate to handle the level of concurrent requests.

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

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.

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. Do not use UDP, however, if remote clients are using the service.

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.

- 5 Click Save.

Managing NFS Service

This section tells you how to perform day-to-day management tasks for NFS service once you have it up and running.

Stopping NFS Service

When the server starts up, a startup script checks to see if any NFS exports have been defined; if so, NFS starts automatically.

If NFS is not running and you add exports, wait a few seconds for the service to launch. When the service is running, a globe appears on the service icon.

To stop NFS service:

- Delete all exports.

The globe on the service icon disappears. However, the `nsfd` daemons continue to run until the server is restarted.

Viewing NFS Service Status

You use Server Status to check the status of all Mac OS X Server devices and services.

To view NFS service status:

- In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select NFS in the list of services under the server name.

If the services aren't visible, click the arrow to the left of the server name.

The Overview tab tells you whether or not the service is running and if `mountd`, `nsfd`, and `portmap` process are running.

The `mountd` process handles mount requests from client computers (only one `mountd` process will appear in the status window if you've defined any exports).

The `nsfd` process responds to read/write requests from client computers that have mounted folders.

The `portmap` process allows client computers to find `nfs` daemons (always one process).

Viewing Current NFS Exports

You can use the Terminal application to view a list of the current NFS exports.

To view current NFS exports:

- In Terminal, enter “showmount -e”.

If this command does not return results within a few seconds, there are no exports and the process is blocked (hung). Press Control-C to exit the showmount command and return to an active command line in your Terminal window.

Supporting Client Computers

This section describes the client computer requirements for using Mac OS X file services.

Supporting Mac OS X Clients

Apple file service requires the following Mac OS X system software:

- Mac OS X version 10.2
- TCP/IP connectivity
- AppleShare 3.7 or later

Go to the Apple support Web site at www.apple/support/ to find out the latest version of AppleShare client software supported by Mac OS X.

Connecting to the Apple File Server in Mac OS X

You can connect to Apple file servers by entering the DNS name of the server or its IP address in the Connect to Server window, or, if the server is registered with Network Service Location, you can select its name in the list of servers there.

Note: Apple file service does not support AppleTalk connections, so clients need to use TCP/IP to access file services. You can use AppleTalk to find Apple file servers, but the connection must be made using TCP/IP.

To connect to the Apple file server in Mac OS X:

- 1 In the Finder, choose “Connect to Server” from the Go menu.
- 2 In the Connect to Server pane, do one of the following:

Select the name of the server in the list (if it appears there).

Type the DNS name of the server in the Address field. You can enter DNS names in any of the following forms:

dns

afp://dns

afp://dns/sharepoint

Type the server’s IP address in the Address field.

- 3 Click Connect.
- 4 Enter your user name and password, then click Connect.
- 5 Select the server volume you want to use and click OK.

Setting Up a Mac OS X Client to Mount a Share Point Automatically

As an alternative to using the automount feature of Apple file service, FTP, or NFS, Mac OS X clients can set their computers to mount server volumes automatically.

To set a Mac OS X client computer to mount a server volume automatically:

- 1 Choose Connect to Server from the Finder's Go menu to mount the volume on the client computer.
- 2 Open System Preferences and select the Login pane.
- 3 Click Add, then locate the Recent Servers folder and double-click the volume you want automatically mounted.

The volume is added to the list of items in the Recent Servers folder in the user's home Library folder.

When the client user logs in the next time, the server—if available—will be mounted automatically.

The client user can also add the server volume to Favorites and then use the item in the Favorites folder in the home Library.

Changing the Priority of Network Connections

Mac OS X uses its *multihoming* capabilities to support multiple network connections. When more than one connection is available, Mac OS X selects the best connection according to the order you specify in the Network preferences.

To change the priority of network connections:

- 1 Open the Network pane of System Preferences.
- 2 Choose a configuration set from the Location menu if you have configurations set up, or use Automatic.
- 3 Choose Active Network Ports from the Show pop-up menu.
- 4 Drag the connections in the Active Ports list into the desired order.

Mac OS X uses the first available connection from the top of the list.

Supporting Mac OS 8 and Mac OS 9 Clients

Apple file service requires the following Mac OS 8 or 9 system software:

- Mac OS 8 (version 8.6) or Mac OS 9 (version 9.2.2)

- TCP/IP
- AppleShare 3.7 or later

Go to the Apple support Web site at www.apple.com/support/ to find out the latest version of AppleShare client software supported by Mac OS 8 and Mac OS 9.

Connecting to the Apple File Server in Mac OS 8 or Mac OS 9

Apple file service does not support AppleTalk connections, so clients need to use TCP/IP to access file services. You can use AppleTalk to find Apple file servers, but the connection must be made using TCP/IP.

To connect to the Apple file server in Mac OS 8 or Mac OS 9:

- 1 Open the Chooser and click Server IP Address.
- 2 Enter the IP address or the name of the server in the window that appears and click Connect.
- 3 Enter your user name and password, then click Connect.
- 4 Select the volume you want to use and click OK.

Setting up a Mac OS 8 or Mac OS 9 Client to Mount a Share Point Automatically

As an alternative to using the automount feature of AFP, FTP, or NFS, clients can set their computers to mount server volumes automatically.

To set a Mac OS 8 or Mac OS 9 client computer to mount a server volume automatically:

- 1 Use the Chooser to mount the volume on the client computer.
- 2 In the select-item dialog that appears after you log in, check the server volume you want to mount automatically.

Supporting Windows Clients

Mac OS X Server supports the native Windows file sharing protocol, Server Message Block (SMB). SMB is also known as Common Internet File System (CIFS). Mac OS X Server comes with built-in browsing and name resolution services for your Windows client computers. You can enable Windows Internet Naming Service (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. You do not 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.

See “Ensuring the Best Cross-Platform Experience” on page 236 for information about setting up a dedicated share point for Windows users, and “Windows User Password Validation” on page 236 for information about different techniques of validating Windows user passwords.

TCP/IP

In order to have access to Windows services, Windows client computers must be properly configured to connect over TCP/IP. See your Windows networking documentation for information on TCP/IP configuration.

Using the Network Neighborhood to Connect to the Windows Server

Before trying to connect to the server from a Windows client computer, find out the workgroup or domain of both the client computer and the file server.

You can find the workgroup name of a Windows client computer in the computer’s Network Neighborhood window.

To find the server’s workgroup name, click the File & Print tab in Server Settings, then click Windows and choose Configure Windows Services.

To connect to a Windows server using the Network Neighborhood:

- 1 On the Windows client computer, open the Network Neighborhood window. If you are in the same workgroup or domain as the server, skip to step 4.
- 2 Double-click the Entire Network icon.
- 3 Double-click the icon of the workgroup or domain the server is located in.
- 4 Double-click the server’s icon.
- 5 Log in using your Windows login name.

Connecting to the Windows Server Without the Network Neighborhood

You can connect to the Windows server by double-clicking its name in the Network Neighborhood. You can also connect without using the Network Neighborhood.

To connect to the Windows server without the Network Neighborhood:

- 1 On the Windows client computer, choose Find from the Start menu, then choose Computer from the submenu.
- 2 Type the name or IP address of your Windows server.
- 3 Double-click the server to connect.
- 4 Log in using your Mac OS X Server login name.

Supporting NFS Clients

Consult your UNIX documentation or system administrator for information on managing mounts.

Solving Problems With File Services

Solving Problems With Apple File Service

User Can't Find the Apple 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.

User Can't Connect to the Apple 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.
- Verify that logging in is enabled for the user in the Users & Groups module of Workgroup Manager.
- 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. Administrators who want to use the admin password to log in as a user need at least AppleShare 3.8.5.
- 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 Chapter 15, "Firewall Service."

User Doesn't See Login Greeting

- Upgrade the software on the user's computer. Apple file service client computers must be using Appleshare client software version 3.7 or later.

Solving Problems With Windows Services

User 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.

User Can’t Log in to the Windows Server

- If you are using Password Server to authenticate users, check to make sure that it is configured correctly. See “Setting Up an Open Directory Domain and Password Server” on page 92.
- If you have user accounts created in a previous version of Mac OS X Server (version 10.1 or earlier) that are still configured to use Authentication Manager, make sure that Authentication Manager is enabled. Then reset the passwords of existing users who will be using Windows services. Reset the user’s password and try again. See *Understanding and Using NetInfo* for information on how to use the command line utilities to configure Authentication Manager. This document is available on the Mac OS X Server Web site: www.apple.com/macosx/server/

Solving Problems With File Transfer Protocol (FTP)

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 Settings, 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 “Port Reference” on page 540.

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.

Anonymous FTP Users Can’t Connect

- Verify that anonymous 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.

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

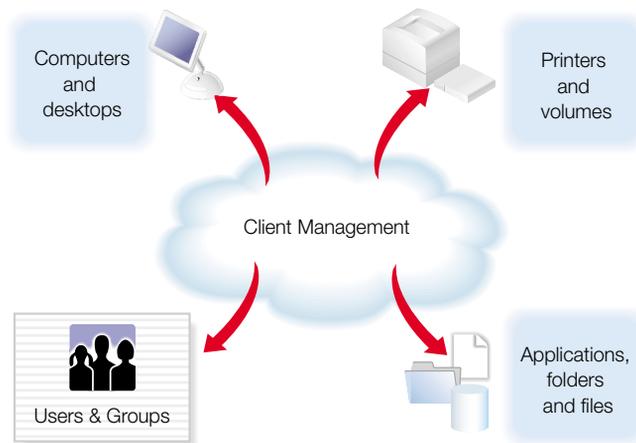
To obtain the UNIX manual pages for FTP, open the Terminal application in Mac OS X. At the prompt, type “man ftp” and press the Return key.

- *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.

Client Management: Mac OS X

Workgroup Manager provides network administrators with a centralized method of managing Mac OS X workstations, controlling access to software and removable media, and providing a consistent, personalized experience for users at different levels, whether they are beginners in a classroom or advanced users in an office. Mac OS X Server saves user documents and preferences in a home directory, so your users can access their files from any Mac on your network. Using Workgroup Manager, you can create user accounts, and then set up groups to provide convenient and efficient access to resources. You can also use account settings and managed preferences to allow more or less flexibility to suit the level of administrative control you want or need.

User management is the result of combining a user's individual settings and preferences, plus settings and preferences for the workgroup and computer he or she is using. The term *managed client* refers to a user, group, or computer whose access privileges and/or preferences are under administrative control. Managing clients gives you control over user access to applications, removable media, printers, computers, and system resources.



This chapter summarizes certain aspects of Mac OS X client management, describes how to set up Mac OS X computer accounts using Workgroup Manager, and gives details about using managed preferences to customize and control the Mac OS X user experience. You'll learn how to

- use Workgroup Manager to control user settings and privileges
- set up and manage computer accounts
- manage preference settings for users, groups, and computer accounts
- set up and manage mobile computers

Important If you need to manage Mac OS 9 or Mac OS 8 clients, read Chapter 10, “Client Management: Mac OS 9 and OS 8.”

Transition Strategies for Mac OS X Client Management

If you currently manage your Mac OS 9 or Mac OS 8 clients using Macintosh Manager and you want to upgrade to Mac OS X, download “Upgrading to Mac OS X Server” from the Web site listed below:

www.apple.com/macosx/server/

The User Experience

This section describes both the actual user experience and the server processes for Mac OS X managed clients.

Logging In

When a managed client computer starts up, a login dialog box appears. Depending on the login settings selected, a user either types his or her user name or chooses it from a list. The user name and password are verified by directory services, and then the server returns a list of workgroups for that user and the user selects a workgroup. The user's environment, privileges, and preferences are determined by the settings chosen for that user, the selected workgroup, and the computer he or she uses.

When you create user accounts, the login settings determine the user experience. If you allow simultaneous login, the user can log in to more than one computer.

Note: Simultaneous login is not recommended for most users. You may want to reserve simultaneous login privileges only for technical staff, teachers, or other users with administrator privileges.

Locating the Home Directory

User documents are stored in a user's home directory, which users can access by clicking the Home icon in a Finder window's toolbar. For more about home directories see Chapter 3, “Users and Groups.”

Before You Begin

You should consider taking advantage of client management if

- you want to provide users with a consistent, controlled interface while allowing them to access their documents from any computer
- you want to control privileges on mobile computers
- you want to reserve certain resources for only specific groups or individuals
- you need to secure computer usage in key areas such as administrative offices, classrooms, or open labs

Before you set up computer accounts or managed preferences for users, groups, or computers, be sure you follow these preliminary steps.

Step 1: Make sure your computers meet minimum requirements

Client Computer Software Requirements

- Mac OS X v. 10.2 as the primary operating system

Note: Workgroup Manager is not used to manage Mac OS 9 or Mac OS 8 clients.

Client Computer Hardware Requirements

- Macintosh computer with a G3 processor or better (except original PowerBook G3 or upgraded PowerPC processors)
- 128 megabytes (MB) of physical random access memory (RAM)
- 1.5 gigabytes (GB) of disk space available

Administrator Computer Software Requirements

- Mac OS X Server v. 10.2 installed

Administrator Computer Hardware Requirements

- Macintosh computer with a G3 processor or better (except original PowerBook G3 or upgraded PowerPC processors)
- 128 MB of RAM
- 4 GB of available disk space

Step 2: Create a shared domain to store account information

Use Open Directory Assistant to set up a shared domain where you can store user, group, and computer account information. For more information about domain hierarchies and how to use Open Directory Assistant, see Chapter 2, “Directory Services.”

Step 3: Make sure users and their home directories exist

Use Workgroup Manager to set up user accounts and home directories. Once users are created in Workgroup Manager, they are ready to be managed on Mac OS X clients. You can set up various privileges (such as print or mail quotas) for users as you create them.

Home directories can be stored on an Apple Filing Protocol (AFP) server. You can set up group volumes as AFP share points and add additional share points if you need them. Each user you want to manage must have a home directory. If no home directory exists for a user, he or she cannot log in.

See Chapter 3, “Users and Groups,” for information about how to create users, define user privileges, and set up home directories.

Designating Administrators

For Mac OS X clients, the server administrator has the greatest amount of control over other users and their privileges. The server administrator can create users, groups, and computer accounts and assign settings, privileges, and managed preferences for them. He or she can also create other server administrator accounts, or give some users (for example, teachers or technical staff) administrative privileges within certain directory domains. These “directory domain administrators” can manage users, groups, and computer accounts within the limits assigned to them by the server administrator.

For more information about assigning administrative privileges to users with network accounts, see Chapter 3, “Users and Groups.”

Setting Up User Accounts

If you use Workgroup Manager to manage your OS X clients, you can set some privileges when you set up accounts. You can use “presets” like templates and apply various settings automatically when you create an account. See Chapter 3, “Users and Groups,” for more information about how to set up user accounts.

Depending on your needs, you may want to set up local user accounts in addition to network user accounts. A network user has a user account associated with Mac OS X Server and you can allow that user to log in from various computers on your network. A local user has an account associated with a specific client computer, and his or her local account is independent from any network user account and other local accounts on other computers. An individual user may have both a network account that provides access to network services and a separate local account on a specific computer. You can set up managed preferences for any user with a network account, but the most convenient way to manage network users is by managing preferences for groups to which they belong. This makes it easier to manage users regardless of which computer they use.

If users have local accounts on specific computers, you can still manage their user preferences on the client computer without using Workgroup Manager. However, it may be more useful to manage local users indirectly by using Workgroup Manager to manage preferences for the client computer and group that can access that computer. These group and computer preferences are cached for offline use, making this preference configuration especially useful for mobile computers. If a user on a mobile computer disconnects from the network, he or she is still managed.

You can set up managed preferences for users after you create the user accounts. For more information about managed preferences and how to use them, see “Managing Preferences” on page 282.

Setting Up Group Accounts

Although Mac OS X users are not required to be added to group accounts in order to be managed, groups are still very important for efficient and effective client management. For example, you can use groups to provide users with the same access privileges to media, printers, and volumes.

For more information about how to create group accounts using Workgroup Manager, see “Administering Group Accounts” on page 165.

Managed preferences assigned to a particular group apply to all users in that group. However, managed user preferences may take precedence over group preferences. You can set up managed preferences for groups after you create the group account. For more information about how to manage preferences, see “Managing Preferences” on page 282.

Setting Up Computer Accounts

A computer account is a list of computers that have the same preference settings and are available to the same users and groups. You can create and modify computer accounts in Workgroup Manager. Computer accounts that you set up appear in the list on the left side of the window. The list of computer accounts is searchable. Settings appear on the List, Access, and Cache panes on the right side of the window.

When you set up a computer account, make sure you have already determined how computers will be identified. Use descriptions that are logical and easy to remember (for instance, the description might be the computer name). You must use the “on board” or built-in Ethernet address for a computer’s Address information. This information is unique to each computer. The client computer uses this data to find preference information when a user logs in. You can browse for a computer and Workgroup Manager will enter the computer’s Ethernet address and name for you.

When a computer starts up, it checks directory services for a computer account record that contains its Ethernet address and uses settings for that computer account. If no record is found, the computer uses settings for the Guest Computers computer account.

You can set up managed preferences for users after you create the user account. For more information about managed preferences and how to use them, see “Managing Preferences” on page 282.

If you want a directory domain administrator to edit computer accounts, add or delete computers from a list, or edit computer account preferences, you must give that administrator those privileges. You can assign an administrator privileges for all computer accounts or for a set of specific computer accounts. For more information about assigning administrative privileges, see Chapter 3, “Users and Groups.”

Creating a Computer Account

You can use a computer account to assign the same privileges and preferences to multiple computers. You can add up to 2000 computers to a computer account.

To set up a computer list:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to open the directory domain where you want to store the new account, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Click New Record, then type in a list name.
- 6 To add a computer to the list, click Add and type the computer’s Ethernet address in the Address field.

Alternatively, you can click Browse, and Workgroup Manager will enter the computer’s Ethernet address and name for you.

- 7 Type a description, such as the computer name.
- 8 Type a comment.

Comments are useful for providing additional information about a computer’s location, configuration (for example, a computer set up for individuals with special needs), or attached peripherals. You could also use the comment for additional identification information, such as the computer’s model or serial number.

- 9 Continue adding computers until your computer list is complete.
- 10 Save the account.

Note: Computers cannot belong to more than one list, and you cannot add computers to the Guest Computers account.

Creating a Preset for Computer Accounts

You can select settings for a computer account and save them as a “preset.” Presets work like templates, allowing you to apply preselected settings and information to a new account. Using presets, you can easily set up multiple computer accounts with similar settings. You can use presets only during account creation. You cannot use a preset to modify an existing computer account.

To set up a preset for computer accounts:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to open the directory domain where you want to create computer accounts using presets, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 To create a new preset from a blank account, first create a new computer account. To create a preset using data in an existing computer account, open the account.
- 6 In each settings pane, fill in the information you want to use in the preset.
- 7 Choose Save Preset from the Presets pop-up menu.

After you create a preset, you can no longer change its settings, but you can delete it or change its name.

To change a preset’s name, choose the preset from the Presets pop-up menu, then choose Rename Preset.

To delete a preset, choose a preset from the Presets pop-up menu, then choose Delete Preset.

Using a Computer Accounts Preset

When you create a new computer account, you can choose any preset from the Presets pop-up menu to apply initial settings, but you can still change the account settings to meet your needs. Until you save account information, changing to a different preset overwrites earlier information. Once the account is saved, the Preset menu dims and cannot be used again for that account.

To use a preset for computer accounts:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to open the directory domain where you want to store the new account, then click Accounts.

- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Choose the preset you want to use from the Presets pop-up menu.
- 6 Create a new account.
- 7 Add or update settings as needed, then save the account.

Adding Computers to an Existing Computer Account

You can easily add more computers to an existing list. However, you cannot add computers to the Guest Computers list.

To add additional computers to a list:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Select the account to which you want to add computers.
- 6 If you are using presets, select the one from the Presets pop-up menu.
- 7 Click Add, then type the computer's Ethernet address in the Address field.

Alternatively, you can click Browse, and Workgroup Manager will enter the computer's Ethernet address and name for you.

- 8 Type a description, such as the computer name.
- 9 Type a comment.

Comments are useful for providing additional information about a computer's location, configuration (for example, a computer set up for individuals with special needs), or attached peripherals. You could also use the comment for additional identification information, such as the computer's model or serial number.

- 10 Click Save.
- 11 Continue adding computers and information until your list is complete.

Editing Information About a Computer

After you add a computer to a computer account, you can edit information when necessary.

To change computer information:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Select a computer account.
- 6 In the List pane, select the computer whose information you want to edit, and click Edit.
- 7 Change information in the information fields as needed.

Moving a Computer to a Different Computer Account

Occasionally, you may want to group computers differently. Workgroup Manager lets you conveniently move computers from one list to another.

Computers cannot belong to more than one list, and you cannot move computers to the Guest Computers account.

To move a computer from one list to another:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Select a computer account.
- 6 In the List pane, select the computer you want to move, and click Edit.
- 7 Select a new computer account in the “Move to list” pop-up menu, and click OK.

Deleting Computers From a Computer List

When you delete a computer from a computer account, that computer is no longer managed.

To delete a computer from a list:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Select a computer account.

- 6 In the List pane, select one or more computers in that account's computer list.
- 7 Click Remove.

Deleting a Computer Account

If you no longer need an entire computer account, you can delete it. You cannot delete the Guest Computers account.

To delete a computer account:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab, then click List.
- 5 Select a computer account.
- 6 Choose "Delete Selected Computer List" from the Server menu.

Searching for Computer Accounts

Workgroup Manager has a search feature that allows you to find specific computer accounts quickly. You can search within a selected domain and filter search results.

To search for computer accounts:

- 1 Open Workgroup Manager.
- 2 Click the lock and enter your user name and password.
- 3 Click Accounts, then click the Computers tab.
- 4 Using the At pop-up menu below the computer accounts list, limit your search to one of the following locations:

Local Directory: Search for account records on local volumes only.

Search Path: Search for account records using the path defined in Directory Setup for the computer where you are logged in (for example, myserver.mydomain.com).

Other: Browse and select an available directory domain to search for account records.

- 5 Select an additional filter from the filter pop-up menu next to the search field, if you wish.
- 6 Type search terms in the search field, then press Return.

Managing Guest Computers

If an unknown computer (one that isn't already in a computer account) connects to your network and attempts to access services, that computer is treated as a "guest." Settings chosen for the Guest Computers account apply to these unknown or "guest" computers.

Using the Guest Computers account is not recommended for large numbers of computers. Most of your computers should belong to regular computer lists.

During server software installation, a guest computer record is automatically created only in the original directory domain. Afterward, a server administrator can create additional guest computer accounts in other directory domains. After the account is created, "Guest Computers" appears in the list of computer accounts.

Each directory domain can have only one guest computer account. Depending on network organization and setup, you may not be able to create a guest computer account in certain directory domains.

Note: You cannot add or move computers to the Guest Computers account, and you cannot change the list name.

To set up the Guest Computers account:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the guest computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab.
- 5 Select Guest Computers in the account list.
- 6 Click List, then select a Preferences settings.

Select Enable if you want to set up managed preferences. If you select this option, you should click Cache, and then set how often you want to update preferences.

Select Inherit if you want guest computers to have the same managed preference settings as the parent server.

- 7 Click Access and select the settings you want to use.
- 8 Click Cache and set an interval for clearing the preferences cache, then click Save.

After you set up the Guest Computers account, you can manage preferences for it if you wish. For more information about using managed preferences, see "Managing Preferences" on page 282.

If you do not select settings or preferences for the Guest Computers account, guest computers are not managed. However, if the person using the computer has a Mac OS X Server user account with managed user or group preferences, those settings still apply when the user connects to your network and logs in.

If the user has an administrator account on the computer, he or she can choose not to be managed at login. Unmanaged users can still use the “Go to Folder” command to access a home directory on the network.

To delete the Guest Computers account, select the account in the list of computer accounts, then choose Delete from the Edit menu.

Working With Access Settings

Settings in the Access pane let you make computers in a list available to users in groups. You can allow only certain groups to access computers in a list, or you can allow all groups (and therefore, all users) to access the computers in a list. You can also control certain aspects of local user access.

Restricting Access to Computers

You can reserve computers so that only certain users have access to them. This can make it easier to provide access to limited resources. For example, if you have two computers set up with the appropriate hardware and software needed to import and edit video, you can reserve those computers for users who need to do video production. First, make sure the user accounts exist, then add the users to a “video production” group, then give only that group access to your video production computers.

Note: A user with a local administrator account may always log in.

To reserve computers for specific groups:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab.
- 5 Select a computer account, then click Access.
- 6 Select “Restrict to groups below.”
- 7 Click Add, then select one or more groups and drag them to the list.

To remove an allowed group, select it and click Remove.

Making Computers Available to All Users

If you want, you can make computers in a list available to any user in any group account you set up.

To make computers available to all users:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab.
- 5 Select a computer account, then click Access.
- 6 Select “All groups can use the computer.”

Using Local User Accounts

Local accounts are useful for both stationary and mobile computers with either single or multiple users. Anyone with a local administrator account on a client computer can create local user accounts using the Accounts pane of System Preferences. Local users authenticate locally.

If you plan to supply individuals with their own portable computers (iBooks, for example), you may want to make the user a local administrator for the computer. A local administrator has more privileges than a local or network user. For example, a local administrator can add printers, change network settings, or select not to be managed.

The easiest way to manage preferences for local user accounts is to manage preferences for the computer that has those local accounts and for the workgroups assigned to the computer.

To provide access for users with local accounts:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Accounts.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab.
- 5 Select a computer account that contains computers with local users, then click Access.
- 6 The account you select must allow local users to log in. Make sure “Allow users with local-only accounts” is selected.
- 7 If you want local users to see a list of all available workgroups during login, select “All groups can use the computer.”

- 8 If you want to show only certain workgroups to users during login, select “Restrict to groups below,” and add groups to the list.
- 9 Click Save.

Managing Portable Computers

It is important to plan how you want to manage portable computers that have access to your network. This section gives suggestions for managing portable computers used by either multiple users or an individual user.

Unknown Portable Computers

To manage users who have their own personal portable computers running Mac OS X system software, you can use the Guest Computers account to apply computer-level management for unknown or “guest” computers on your network. If these users log in using a Mac OS X Server user account, user and group managed preferences and account settings also apply.

For more information about setting up the Guest Computers account for Mac OS X users, see “Managing Guest Computers” on page 277. For information about managing unknown portable computers that use Mac OS 9 or OS 8 system software, see “Providing Quick Access to Unimported Users” on page 429.

Portable Computers With Multiple Local Users

One example of shared portable computers is an iBook Wireless Mobile Lab. An iBook Wireless Mobile Lab contains either 10 or 15 student iBooks (plus an additional iBook for an instructor), an Airport base station, and a printer, all on a mobile cart. The cart lets you take the computers to your users (for example, from one classroom to another).

To manage the iBooks on your cart, create identical generic local user accounts on each computer (for example, all the accounts could use “Math” as the user name and “student” as the password). You might want to create different generic local accounts for different purposes, such as one for a History class, one for a Biology class, and so on. Each account should have a local home directory and should not have administrative privileges. Use a separate local administrator account on each computer to allow server administrators (or other individuals) to perform maintenance tasks and upgrades, install software, and administer the local user accounts.

After creating the local user accounts, add each of the computers to a computer list, then manage preferences for that list. Because multiple users can store items in the local home directory for the generic account, you may want to periodically clean out that folder as part of your maintenance routine.

Portable Computers With One Primary Local User

There are two ways set up portable computers for a single user.

- The user does not have administrator privileges, but has a local account.
Set up a local administrator account on the computer (do not give the user information about this account), then set up a local account for the user. Users with local accounts that do not have administrator privileges cannot install software and can only add or delete items in their own home directories. A local user can share items with other local users by using the Public folder in his or her local home directory.
- The user is the administrator for the computer.
If the user is the local administrator, he or she can choose during login whether or not to be managed. For example, in order to access servers at school, the user should choose to be managed at login, but at home he or she may prefer not to be managed since access to the school servers may not be available.
If the user also has a Mac OS X Server user account and network access is available, it may still be preferable to log in using the local account in order to reduce network traffic. The user can connect to his or her network home directory (to store or retrieve documents, for example) via the “Go to Folder” command in the Finder’s Go menu.

Using Wireless Services

You can provide wireless network service to managed clients using AirPort, for example. When a user with a portable computer leaves the wireless area or changes to a different network directory server (by moving out of one wireless area and into another), client management settings may be different. Users may notice that some network services, such as file servers, printers, shared group volumes, and so forth, are unavailable from the new location. Users can purge these unavailable resources by logging out and logging in again.

If you need more information about using AirPort, consult AirPort documentation or visit the Web site:

www.apple.com/airport/

How Workgroup Manager Works With System Preferences

Workgroup Manager allows administrators to set and lock certain system settings for users on their network. You can set preferences once and allow users to change them, you can keep preferences under administrative control at all times and allow no user changes, or you can choose not to impose any settings at all.

In addition to various settings for users, groups, and computer accounts, Workgroup Manager provides control over these preferences:

Preference pane	What you can manage
Applications	Applications and system preferences available to users
Classic	Classic startup settings, sleep settings, and the availability of Classic items such as Control Panels
Dock	Dock location, behavior, and items
Finder	Finder behavior, desktop appearance and items, and availability of Finder menu commands
Internet	Email account preferences and Web browser preferences
Login	Login window appearance and items that open automatically when a user logs in
Media Access	Settings for CDs, DVDs, and recordable discs, plus settings for internal and external disks such as hard drives or floppy disks
Printer	Available printers and printer access

Managing Preferences

In Workgroup Manager, information about users, groups, and computer accounts is integrated with directory services. Once you've set up users, groups, and computer accounts, you do not have to import them into a separate tool in order to manage them on Mac OS X client computers.

Managing preferences means you can control settings for certain system preferences in addition to controlling user access to system preferences, applications, printers, and removable media. Workgroup Manager stores information about settings and preferences in user, group, or computer records on the Mac OS X server. Group preferences are stored on the group volume. User preferences are stored in the user's home directory (the Home folder on Mac OS X clients).

After user, group, and computer accounts are created, you can start managing preferences for them using the Preferences pane in Workgroup Manager. To manage preferences for Mac OS X clients, you must make sure each user you want to manage has a home directory. If a user doesn't have a home directory, he or she will not be able to log in. For information about how to set up a group volume or how to set up home directories for users, see Chapter 3, "Users and Groups."

About the Preferences Cache

Only local user accounts use a preference cache. The preference cache is created on the local hard drive when a user logs in. The cache stores only preferences for the computer account to which that computer belongs and preferences for groups associated with that computer, but this can influence how a user is managed offline.

The cached preferences can help you manage local user accounts on portable computers even when they are not connected to a network. For example, you can create an account for the set of computers you want to manage, and then manage preferences for the computer accounts. Next, make these computers available to groups, then manage preferences for the groups. Finally, set up local user accounts on the computers, and associate those users with the groups you already manage. Now, if a user goes offline or disconnects from your network, he or she is still managed by the computer and group preferences in the cache.

Updating the Managed Preferences Cache

You can update a user's managed preference cache regularly. This setting applies only to computer accounts. The computer checks the server for updated preferences according to the schedule you set.

To set an update interval for the managed preferences cache:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want to modify, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab and select a computer account in the list.
- 5 Click Cache.
- 6 Type in a number representing how frequently you want to update the cache, then choose an update interval (seconds, minutes, hours, days, or weeks) from the pop-up menu. For example, you could update the cache every 5 days.

Updating Cached Preferences Manually

When you need to, you can manually update the managed preferences cache for every computer in a selected computer list. When the cache is updated manually, it will not be updated again automatically until the set interval has passed.

To update the managed preferences cache:

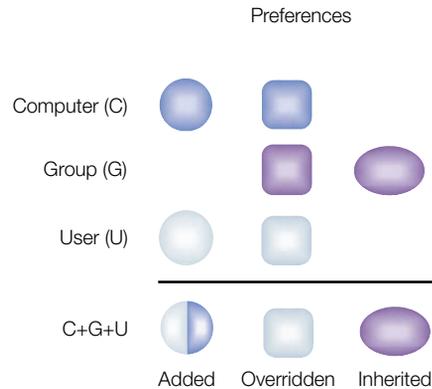
- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the computer account you want, then click Preferences.

- 3 Click the lock and enter your user name and password.
- 4 Click the Computers tab and select a computer account from the list.
- 5 Click Cache, then click “Update the Cache.”

How Preference Management Works

Managed preference settings can be applied to user, group, or computer accounts. The final set of preferences a user has is a combination of preference settings for his or her own user account, preferences for the workgroup chosen at login, and preferences for the computer he or she is currently using.

For some preferences, such as Finder preferences, user settings override group settings and group settings override computer settings. Other preferences, such as printer preferences, have an additive result. For example, the final list of printers available to a user is a combination of the computer printer list, the group printer list, and the user’s printer list. Preferences for applications, Dock items, and login items behave in a similar manner.



In some cases, you may find it easier and more useful to set certain preferences for only one type of record. For example, you could set printer preferences only for computers, set application preferences only for workgroups, and set Dock preferences only for users. In such a case, no override or addition occurs for these preferences because the user inherits them without competition.

Preference Management Options

When you manage preferences for a user, group, or computer account, you can choose to set the preferences once, always, or never using radio buttons in the management bar.

Managing a Preference Once

If you want to manage a preference initially for users, but allow them to make changes if they have that privilege, select Once in the management bar. When a user logs in, preference files in his or her home directory are updated with any preferences that are managed “once.” These preference files are time stamped. If you update settings for a preference that is managed once, Workgroup Manager applies the most recent version to the user’s preference files the next time he or she logs in.

For some preferences, such as Classic preferences or Media Access preferences, Once is not available. You can only select Never or Always.

Always Managing a Preference

You can force preference settings for a user by selecting Always in the management bar. The next time the user logs in, the preference reverts to the original settings chosen by the administrator even if the user is allowed to change the settings. Preferences that are “always” managed are stored in the /Library/Managed Preferences folder.

Never Managing a Preference

If you don’t want to manage settings for a preference at all, select Never in the management bar. If you provide users with access to an unmanaged preference, they can change settings as they wish.

“Never” is the default setting for all preferences.

Managing User Preferences

You can manage preferences for individual users as needed. However, if you have large numbers of users, it may be more efficient to manage most preferences by group and computer instead. You might want to manage preferences at the user level only for specific individuals, such as directory domain administrators, teachers, or technical staff.

You should also consider which preferences you want to leave under user control. For example, if you aren’t concerned about where a user places the Dock, you might want to set Dock Display management to Never.

To manage user preferences:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the user account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Click the Users tab and select a user account in the account list.
- 5 Click the icon for the preference you want to manage.

- 6 In each tab for that preference, choose a management setting. Then select preference settings or fill in information you want to use.

Some management settings are not available for some settings, and some preferences are not available to some types of accounts. Two preferences (Printing and Media Access) allow only one management setting that applies to all options for that preference.

- 7 When you are finished, click Apply Now.

Managing Group Preferences

Group preferences are shared among all users in the group. Setting some preferences only for groups instead of for each individual user can save space, especially when you have large numbers of managed users.

Because users can select a workgroup at login, they have the opportunity to choose a group with managed settings appropriate to the current task, location, or environment. It can be more efficient to set preferences once for a single group instead of setting preferences individually for each member of the group.

To manage group preferences:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the group account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a group account in the account list.
- 5 Click the icon for the preference you want to manage.
- 6 In each tab for that preference, choose a management setting. Then select preference settings or fill in information you want to use.

Some management settings are not available for some settings, and some preferences are not available to some types of accounts. Two preferences (Printing and Media Access) allow only one management setting that applies to all options for that preference.

- 7 Click Apply Now.

Managing Computer Preferences

Computer preferences are shared among all computers in a list. In some cases, it may be more useful to manage preferences for computers instead of for users or groups.

To manage computer preferences:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the user account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a computer account in the account list.
- 5 In each tab for that preference, choose a management setting. Then select preference settings or fill in information you want to use.

Some management settings are not available for some settings, and some preferences are not available to some types of accounts. Two preferences (Printing and Media Access) allow only one management setting that applies to all options for that preference.

- 6 In each tab for that preference, select the settings you want to use.
- 7 Click Apply Now.

Editing Preferences for Multiple Records

You can edit preference for more than one user, group, or computer account at a time. If some settings are not the same for two or more accounts, you may see a “mixed-state” slider, radio button, checkbox, text field, or list. For sliders, radio buttons, and checkboxes, a dash is used to indicate that the setting is not the same for all selected accounts. For text fields, the term “Varies...” indicates a mixed state. Lists show a combination of items for all selected accounts.

If you adjust a mixed-state setting, every account will have the new setting you choose. For example, suppose you select three group accounts that each have different settings for the Dock size. When you look at the Dock Display preference pane for these accounts, the Dock Size slider is centered and has a dash on it. If you change the position of the Dock Size slider to Large, all selected accounts will have a large-size Dock.

Disabling Management for Specific Preferences

After you set up managed preferences for any account, you can turn off management for specific preference panes by setting the management setting to Never.

To selectively disable preference management:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the icon for a preference that is currently being managed.
- 6 Click the tab containing the preference settings you no longer want to manage.

Two preferences (Printing and Media Access) do not have a management settings bar for each tab. Instead, a management bar is displayed above the tabs.

- 7 Select Never in the management settings bar.
- 8 Click Apply Now.

When you change the preference management settings, the new setting applies to all items in the active preference pane. If you want to disable all preference management for an individual preference (for example, Dock), make sure the management setting is set to Never in each pane of that preference.

Managing Applications Preferences

Use Applications settings to provide access to applications and to select which items appear in System Preferences.

Applications Items Preferences

Applications Items settings let you create lists of “approved” applications users are allowed to open, and you can allow users to open items on local volumes.

Creating a List of Approved Applications

You need to provide access to the applications you want users to open. To do this, use Items settings for the Applications preference and create a list of “approved” applications. If an application is not on the list, a user cannot open it. You can, however, allow applications to open “helper applications” that are not listed.

You can make applications available to multiple users by managing Items settings for the Applications preference for groups or computer accounts. You can also set this preference for individual users.

To add applications to a user’s list:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the Applications preference icon, then click Items.
- 6 Set the management setting to Always.
- 7 Click Add to browse for the application you want, then add it to the list.

To select multiple items, hold down the Command key.

- 8 When you have finished adding applications to the list, click Apply Now.

Preventing Users From Opening Applications on Local Volumes

When users have access to local volumes, they can access applications on the computer's local hard drive, in addition to approved applications on CDs, DVDs, or other external disks. If you don't want to allow this, you can disable local volume access.

To prevent access to local applications:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the Applications preference icon, then click Items.
- 6 Set the management setting to Always.
- 7 Deselect "User can open items on local volumes."
- 8 Click Apply Now.

Managing Application Access to Helper Applications

Sometimes, applications need to use "helper applications" for tasks they cannot complete themselves. For example, if a user tries to open a Web link in an email message, the email application might need to open a Web browser application to display the Web page.

When you make an application list available for users, groups, or computer accounts, you may want to include common helper applications in that list. For example, if you give users access to an email application, you might also want to add a Web browser, a PDF viewer, and a picture viewer to avoid problems opening and viewing email contents or attached files.

When you set up a list of "approved" items in the Applications preference settings, you can choose whether to allow applications to use helper applications that aren't in the "approved" items list.

To manage access to helper applications:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.

- 5 Click the Applications preference icon, then click Items.
- 6 Set the management setting to Always.
- 7 If you have not already created a list of approved applications, do so now.
Click Add to browse for the application you want to add to the list. To remove an application from the list, select it and click Remove. If you want to allow helper applications, be sure those applications are added to the list.
- 8 Select “Allow approved applications to open non-approved applications” to allow access to helper applications. Deselect this option to disable it.
- 9 Click Apply Now.

Applications System Preferences

You can choose which system preferences users see when they open System Preferences.

Managing Access to System Preferences

When you show an item in System Preferences, a user can open the preference, but may or may not be able to change its settings. For example, if you set preference management for the Dock to Always and you make Dock preferences available in System Preferences, a user can view the settings but cannot make any changes.

Some System Preferences may not be available on your administrator computer. You should either install the missing preferences on the administrator computer you are using, or you should use Workgroup Manager on an administrator computer that has those preferences installed.

To manage access to System Preferences:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Applications preference icon.
- 5 Click System Preferences.
- 6 Set the management setting to Always.
- 7 Deselect the Show checkbox for each item you do not want to display in a user’s System Preferences.

Click Show None to deselect every item in the list.

Click Show All to select every item in the list.

- 8 Click Apply Now.

Managing Classic Preferences

Classic Preferences are used to set Classic startup options, select the Classic System Folder and set sleep options for Classic, and make certain Apple menu items available to users.

Classic Startup Preferences

Startup settings affect what happens when Classic starts.

Making Classic Start Up After a User Logs In

If users often need to work with applications that run in Classic, it is convenient to have Classic start up immediately after a user logs in.

To start Classic after login:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the Classic preference icon, then click Startup.
- 6 Set the management setting to Always.
- 7 Select “Start up Classic on login to this computer.”
- 8 If you don’t want users to see the Classic startup screens, select “Hide Classic while starting.”
- 9 Select “Warn at Classic startup” to show an alert when Classic starts.
- 10 Select “Show Classic in the menu bar” to place a Classic icon in the menu bar.
- 11 Click Apply Now.

Choosing a Classic System Folder

If the name of the hard disk or volume containing the Mac OS 9 System Folder is Macintosh HD, you do not have to specify a Classic System Folder. If you want to use a specific Mac OS 9 System Folder when Classic starts up, you can specify it in the Classic preference pane in Workgroup Manager.

To choose a specific Classic System Folder:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.

- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the Classic preference icon, then click Startup.
- 6 Set the management setting to Always.
- 7 Type in the path to the Classic System Folder you want to use (make certain the path you specify does not contain errors), or use Choose to browse for the folder you want.
- 8 Click Apply Now.

Classic Advanced Preferences

Advanced preference settings for Classic let you control items in the Apple menu, Classic sleep settings, and the user's ability to turn off extensions or rebuild Classic's desktop file during startup.

Allowing Special Actions During Restart

You can allow users to perform special actions, such as turning off extensions or rebuilding Classic's desktop file, when they restart computers. You may want to allow this privilege for specific users, such as members of your technical staff.

To allow special actions during restart:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list.
- 5 Click the Classic preference icon, then click Advanced.
- 6 Set the management setting to Always.
- 7 Select "Allow special startup modes."
- 8 Click Apply Now.

Keeping Control Panels Secure

If you don't want users to have access to Mac OS 9 control panels, you can remove the Control Panels item from the Apple menu.

To prevent access to Control Panels:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Classic preference icon.
- 5 Click Advanced, and set the management setting to Always.
- 6 Select “Hide Control Panels.”
- 7 Click Apply Now.

Preventing Access to the Chooser and Network Browser

If you don't want users to have access to the Chooser or Network Browser in Classic, you can remove these items from the Apple menu.

To remove the Chooser and Network Browser from the Apple menu:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Classic preference icon.
- 5 Click Advanced and set the management setting to Always.
- 6 Select “Hide Chooser and Network Browser.”
- 7 Click Apply Now.

Making Apple Menu Items Available in Classic

You can hide or reveal Apple menu items (other than the Chooser, Network Browser, or Control Panels) as a group. This group includes items such as Calculator, Key Caps, and Recent Applications.

To show other Apple menu items:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Classic preference icon.

- 5 Click Advanced and set the management setting to Always.
- 6 Deselect “Hide other Apple menu items.”
- 7 Click Apply Now.

Adjusting Classic Sleep Settings

When no Classic applications are open, Classic will go to sleep to reduce its use of system resources. You can adjust the amount of time Classic waits before going to sleep after a user quits the last Classic application.

If Classic is in sleep mode, opening a Classic application may take a little longer.

To adjust Classic sleep settings:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Classic preference icon.
- 5 Click Advanced and set the management setting to Always.
- 6 Drag the slider to set how long Classic waits before going to sleep.
If you don't want Classic to go to sleep at all, drag the slider to Never.
- 7 Click Apply Now.

Managing Dock Preferences

Dock settings allow you to adjust the behavior of the user's Dock and specify what items appear in it.

Dock Display Preferences

Dock Display preferences control the Dock's position and behavior.

Controlling the User's Dock

Dock settings allow you to adjust the position of the Dock on the desktop and change the Dock's size. You can also control animated Dock behaviors.

To set how the Dock looks and behaves:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Dock preference icon.
- 5 Click Dock Display.
- 6 Select a management setting (Once or Always).
- 7 Drag the Dock Size slider to make the Dock smaller or larger.
- 8 If you want items in the Dock to be magnified when a user moves the pointer over them, select the Magnification checkbox, then adjust the slider. Magnification is useful if you have many items in the Dock.
- 9 If you don't want the Dock to be visible all the time, select "Automatically hide and show the Dock." When the user moves the pointer to the edge of the screen where the Dock is located, the Dock pops up automatically.
- 10 Select whether to place the Dock on the left, right, or bottom of the desktop.
- 11 Select a minimizing effect.
- 12 If you don't want to use animated icons in the Dock when an application opens, deselect "Animate opening applications."
- 13 Click Apply Now.

Dock Items Preferences

Dock Items settings allow you to add and arrange items in a user's Dock.

Adding Items to a User's Dock

You can add applications, folders, or documents to a user's Dock for easy access.

To add items to the Dock:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Dock preference icon.
- 5 Click Dock Items.
- 6 Select a management setting (Once or Always).

- 7 To add individual applications, regular folders, and documents to the Dock, click Add to browse and select the item you want.

To remove a Dock item, select it and click Remove.

You can rearrange Dock items in the list by dragging them into the order in which you want them to appear. Applications are always grouped at one end; folders and files are grouped at the other.

- 8 When you have finished adding regular and special Dock items, click Apply Now.

Preventing Users From Adding Additional Dock Items

Ordinarily, users can add additional items to their own Docks, but you can prevent this. Users cannot remove Dock items added by the administrator.

To prevent users from adding items to their Docks:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Dock preference icon.
- 5 Click Dock Items, then set the management setting to Always.
- 6 Deselect “Users may add and remove additional Dock items.”
- 7 Click Apply Now.

Managing Finder Preferences

Finder Preferences allow you to control various aspects of Finder menus and windows.

Finder Preferences

Use the Finder Preferences settings in Workgroup Manager to select a Finder type for the user, show or hide items mounted on the desktop, and control Finder window behaviors. You can also make file extensions visible and show users a warning if they attempt to empty the Trash.

Keeping Disks and Servers From Appearing on the User’s Desktop

Normally when a user inserts a disk, that disk’s icon appears on the desktop. Icons for local hard disks or disk partitions and mounted server volumes are also visible. If you don’t want users to see these items on the desktop, you can hide them.

These items still appear in the top-level directory when a user clicks the Computer icon in a Finder window toolbar.

To hide disk and server icons on the desktop:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click the Preferences tab and select a management setting (Once or Always).
- 6 Under “Show these items on the Desktop,” deselect the items you want to hide.
- 7 Click Apply Now.

Controlling the Behavior of Finder Windows

You can select what directory appears when a user opens a new Finder window. You can also define how contents are displayed when a user opens folders.

To set Finder window preferences:

- 1 Open Workgroup Manager and click Preferences.
- 2 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 3 Click the Preferences tab and select a management setting (Once or Always).
- 4 Under “New Finder window shows,” specify the items you want to display.
Select Home to show items in the user’s home directory
Select Computer to show the top-level directory, which includes local disks and mounted volumes.
- 5 Select “Always open folders in a new window” to display folder contents in a separate window when a user opens a folder. Normally, Mac OS X users can browse through a series of folders using a single Finder window.
- 6 Select “Always open windows in Column View” to maintain a consistent view among windows.
- 7 Click Apply Now.

Making File Extensions Visible

A file extension usually appears at the end of a file name (for example, “.txt” or “.jpg”). Applications use the file extension to identify the file type.

To make file extensions visible:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click the Preferences tab and select a management setting (Once or Always).
- 6 Select “Always show file extensions.”
- 7 Click Apply Now.

Selecting the User Environment

You can select either the regular Finder or the Simplified Finder as the user environment. The regular Finder looks and acts like the standard Mac OS X desktop. The Simplified Finder uses panels and large icons to provide users with an easy-to-navigate interface.

To set the user environment:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click the Preferences tab and select a management setting (Once or Always).
- 6 Select either “Use normal Finder” or “Use Simplified Finder to limit access to the computer.”
- 7 Click Apply Now.

Hiding the Alert Message When a User Empties the Trash

Normally, a warning message appears when a user empties the Trash. If you do not want users to see this message, you can turn it off.

To hide the Trash warning message:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click the Preferences tab and select a management setting (Once or Always).
- 6 Deselect “Show warning before emptying the Trash.”
- 7 Click Apply Now.

Finder Commands Preferences

Commands in Finder menus and the Apple menu allow users to easily connect to servers or restart the computer, for example. In some situations, you may want to limit user access to these commands. Workgroup Manager lets you control whether or not certain commands are available to users.

Controlling User Access to an iDisk

If users want to connect to an iDisk, they can use the “Go to iDisk” command in the Finder’s Go menu. If you don’t want users to see this menu item, you can hide the command.

To hide the “Go to iDisk” command:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Commands and set the management setting to Always.
- 6 Deselect “Go to iDisk.”
- 7 Click Apply Now.

Controlling User Access to Remote Servers

Users can connect to a remote server by using the “Connect to Server” command in the Finder’s Go menu and providing the server’s name or IP address. If you don’t want users to have this menu item, you can hide the command.

To hide the “Connect to Server” command:

- 1 Open Workgroup Manager.

- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Commands and set the management setting to Always.
- 6 Deselect “Connect to Server.”
- 7 Click Apply Now.

Controlling User Access to Folders

Users can open a specific folder by using the “Go to Folder” command in the Finder’s Go menu and providing the folder’s path name. If you don’t want users to have this privilege, you can hide the command.

To hide the “Go to Folder” command:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Commands and set the management setting to Always.
- 6 Deselect “Go to Folder.”
- 7 Click Apply Now.

Preventing Users From Ejecting Disks

If you don’t want users to be able to eject disks (for example, CDs, DVDs, floppy disks, or FireWire drives), you can hide the Eject command in the Finder’s File menu.

To hide the Eject command:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.

- 5 Click Commands and set the management setting to Always.
- 6 Deselect Eject.
- 7 Click Apply Now.

Hiding the Burn Disc Command in the Finder

On computers with appropriate hardware, users can “burn discs” (write information to recordable CDs or DVDs). If you don’t want users to have this privilege, you can hide the Burn Disc command in the Finder’s File menu.

To hide the Burn Disc command:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Commands and set the management setting to Always.
- 6 Deselect “Burn Disc.”
- 7 Click Apply Now.

To prevent users from using or burning recordable CDs or DVDs, use settings in the Media Access panes.

Only computers with a CD-RW drive, Combo drive, or Superdrive can burn CDs. The Burn Disc command will work only with CD-R, CD-RW, or DVD-R disks. Only a Superdrive can burn DVDs.

Removing Restart and Shut Down Commands From the Apple Menu

If you don’t want to allow users to restart or shut down the computers they are using, you can remove the Restart and Shut Down commands from the Apple menu.

To hide the Restart and Shut Down commands:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.

- 5 Click Commands and set the management setting to Always.
- 6 Deselect “Restart/Shut Down.”
- 7 Click Apply Now.

As an additional preventive measure, you can also remove the Restart and Shut Down buttons from the login window using settings for Login preferences. See “Managing Login Preferences” on page 305 for instructions.

Finder Views Preferences

Finder Views allow you to adjust the arrangement and appearance of items on a user’s desktop, in Finder windows, and in the top-level directory of the computer.

Adjusting the Appearance and Arrangement of Desktop Items

Items on a user’s desktop appear as icons. You can control the size of desktop icons and how they are arranged.

To set preferences for the desktop view:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Views, then select a management setting (Once or Always). This setting applies to options in all three view tabs.
- 6 Click Desktop View.
- 7 Drag the slider to adjust icon size.
- 8 Select how you want to arrange icons on the user’s desktop.
Select “None” to allow users to place items anywhere on the desktop.
Select “Always snap to grid” to keep items aligned in rows and columns.
Select “Keep arranged by,” then choose a method from the arrangement pop-up menu. You can arrange items by name, creation or modification date, size, or kind (for example, all folders grouped together).
- 9 Click Apply Now.

Adjusting the Appearance of Finder Window Contents

Items in Finder windows can be viewed in a list or as icons. You can control aspects of how these items look, and you can also control whether or not to show the toolbar in a Finder window.

Default View settings control the overall appearance of all Finder windows. Computer View settings control the view for the top-level computer directory showing hard disks and disk partition, external hard disks, mounted volumes, and removable media (such as CDs or floppy disks).

To set preferences for the default and computer views:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Finder preference icon.
- 5 Click Views, then select a management setting (Once or Always). This setting applies to options in all three view tabs.

- 6 Click Default View.
- 7 Drag the Icon View slider to adjust icon size.
- 8 Select how you want to arrange icons.

Select None to allow users to place items anywhere on the desktop.

Select “Always snap to grid” to keep items aligned in rows and columns.

Select “Keep arranged by,” then choose a method from the arrangement pop-up menu. You can arrange items by name, creation or modification date, size, or kind (for example, all folders grouped together).

- 9 Adjust List View settings for the default view.

If you select “Use relative dates,” an item’s creation or modification date is displayed as “Today” instead of “4/12/02,” for example.

If you select “Calculate folder sizes,” the computer calculates the total size of each folder shown in a Finder window. This can take some time if a folder is very large.

Select a size for icons in a list.

- 10 Select “Show toolbar in Finder windows” if you want the user to see the toolbar.

- 11 Click Computer View and adjust Icon View and List View settings for the computer view. Available settings are similar to those available for the default view described in steps 5 through 9.
- 12 Click Apply Now.

Managing Internet Preferences

Internet preferences let you set email and Web browser options.

Setting Email Preferences

Email settings let you specify a preferred email application and supply information for the email address, incoming mail server, and outgoing mail server.

To set email preferences:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Internet preference icon.
- 5 Click Email and select a management setting (Once or Always).
- 6 To set the default email reader, click Set and choose the email application you prefer.
- 7 Type information for the email address, incoming mail server, and outgoing mail server.
- 8 Select an email account type (either POP or IMAP).
- 9 Click Apply Now.

Setting Web Browser Preferences

Use Web settings in Internet preferences to specify a preferred Web browser and a place to store downloaded files. You can also specify a starting point URL for your browser using the Home Page location. Use the Search Page location to specify a search engine URL.

To set Web preferences:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.

- 4 Select a user, group, or computer account in the account list, then click the Internet preference icon.
- 5 Click Web and select a management setting (Once or Always).
- 6 To set the Default Web Browser, click Set and choose a preferred Web browser application.
- 7 Type a URL for the Home Page. This is the page a user sees when a browser opens.
- 8 Type a URL for the Search Page.
- 9 Type a folder location for storing downloaded files, or click Set to browse for a folder.
- 10 Click Apply Now.

Managing Login Preferences

Use Login preferences to set user login options, provide password hints, and control the user's ability to restart and shut down the computer from the login screen. You can also mount the group volume or make applications open automatically after a user logs in.

Login Window Preferences

Login Window settings affect the appearance and function of items in the login window.

Deciding How a User Logs In

Depending on the settings you choose, a user will see either a name and password text field or a list of users in the login window. These settings apply only to computer accounts.

To set up how a user logs in:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a computer account in the account list, then click the Login preference icon.
- 5 Click Login Window and set the management setting to Always.
- 6 Select how the user logs in.

To require the user to type his or her username and password, select "Name and password entry fields."

To allow a user to select his or her name from a list, select "List of users able to access this computer."

- 7 If you decide to use a list of users, select categories of users you want to display in the list.

Select “Show local users” to include local user accounts in the list.

Select “Show network users” to include network users in the list.

Select “Show administrators” to include users with administrator privileges in the list.

If you allow unknown users, you can select “Show other users.”

- 8 Click Apply Now.

Helping Users Remember Passwords

You can use a “hint” to help users remember their passwords. After three consecutive attempts to log in with an incorrect password, a dialog box displays the hint you created.

To show a password hint:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Login preference icon.
- 5 Click Login Window and set the management setting to Always.
- 6 Select “Show password hint after 3 attempts to enter a password.”
- 7 Click Apply Now.

Preventing Restarting or Shutting Down the Computer at Login

Normally, the Restart and Shut Down buttons appear in the login window. If you don’t want the user to restart or shut down the computer, you should hide these buttons.

You may also want to hide the Restart and Shut Down commands in the Finder menu. See “Managing Finder Preferences” on page 296 for instructions. Check the Commands pane of Finder preferences and make sure “Restart/Shut Down” is not selected.

To hide the Restart and Shut Down buttons:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Login preference icon.
- 5 Click Login Window and set the management setting to Always.

- 6 Select “Hide Restart and Shut Down buttons in the Login Window.”
- 7 Click Apply Now.

Login Items Preferences

Settings for Login Items allow you to open applications or mount the group volume automatically for the user.

Opening Applications Automatically After a User Logs In

You can have frequently used applications ready for use shortly after a user logs in. If you open several items, you can hide them after they open. This prevents excess clutter on the user’s screen, but the applications remain open and accessible.

As the listed applications open, they “stack” on top of each other in the Finder. The last item in the list is closest to the front of the Finder. For example, if you have three items in the list and none of them are hidden, the user sees the menu bar for the last item opened. If an application has open windows, they may overlap windows from other applications.

To make applications open automatically:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Login preference icon.
- 5 Click Login Items and select a management setting (Once or Always).
- 6 To add an item to the list, click Add.
- 7 Select the Hide checkbox for any item you don’t want the user to see right away.
The application remains open, but its windows and menu bar remain hidden until the user activates the application (for example, by clicking its icon in the Dock).
- 8 Deselect “User may add and remove additional login items” if you do not want users to have this privilege.
Users cannot remove items added to this list by an administrator, but users can remove items they’ve added themselves.
- 9 To prevent users from stopping applications that open automatically at login, deselect “User may press Shift to keep applications from opening.”
- 10 Click Apply Now.

Managing Media Access Preferences

Media Access preferences let you control settings for and access to CDs, DVDs, the local hard drive, and external disks (for example, floppy disks and FireWire drives).

Media Access Disc Media Preferences

Disc Media settings affect only CDs, DVDs, and recordable discs (for example, a CD-R, CD-RW, or DVD-R). Computers that do not have appropriate hardware to use CDs, DVDs, or recordable discs are not affected by these settings.

Controlling Access to CDs and DVDs

If a computer can play or record CDs or DVDs, you can control what type of media users can access. You cannot restrict access to individual CDs or DVDs or specific items on them. You can, however, choose not to allow any CDs or DVDs. You can also limit access by requiring an administrator's user name and password.

To control access CDs and DVDs:

- 1 Open Workgroup Manager and click Preferences.
- 2 Select a user, group, or computer account in the account list, then click the Media Access preference icon.
- 3 Set the management setting to Always. This setting applies to all Media Access preference options.
- 4 Click Disc Media.
- 5 Choose settings for CDs and CD-ROMs.

Select the Allow checkbox next to CDs & CD-ROMs to let users access music, data, or applications on compact discs.

To restrict access to compact discs, select Require Authentication to require an administrator user name and password.

To prevent access to all compact discs, deselect Allow.

- 6 Choose settings for DVDs.

Select the Allow checkbox next to DVDs to let users access movies and other information on digital video discs.

To restrict access to DVDs, select Require Authentication to require an administrator user name and password.

To prevent access to all DVDs, deselect Allow.

- 7 Click Apply Now.

Controlling the Use of Recordable Discs

If a computer has the appropriate hardware, users can “burn discs” or write information to a recordable disc such as a CD-R, CD-RW, or DVD-R. Users can burn CDs on computers with a CD-RW drive, Combo drive, or Superdrive. Users can burn DVDs only on computers with a Superdrive.

If you want to limit the ability to use recordable media, you can require an administrator’s user name and password. Alternatively, you could allow users to read information on a recordable disc, but not allow them to burn a disc themselves.

To control the use of recordable discs:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Media Access preference icon.
- 5 Set the management setting to Always. This setting applies to all Media Access preference options.
- 6 Click Disc Media.
- 7 Select options for recordable media.

Select the Allow checkbox next to Recordable Discs to let users use a CD-R, CD-RW, or DVD-R disc.

Select the Authentication checkbox to require an administrator password to use the disc.

To prevent users from recording information to compact discs or DVD-R discs, deselect Allow.

- 8 Click Apply Now.

Media Access Other Media Preferences

Settings in the Other Media pane affect internal hard disks and external disks other than CDs or DVDs.

Controlling Access to Hard Drives and Disks

Media Access settings selected in the Other Media pane let you control access to both a computer’s hard disk and any external disks other than CDs and DVDs. If you don’t allow access to external disks, users cannot use floppy disks, Zip disks, FireWire hard drives, or other external storage devices.

To restrict access to internal and external disks:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Media Access preference icon.
- 5 Set the management setting to Always. This setting applies to all Media Access preference options.
- 6 Click Other Media.
- 7 Select options for Internal Disks (the computer's hard disk and disk partitions).
Select the Authentication checkbox to require a password to access the hard disk.
Deselect the Allow checkbox to prevent users access to the hard disk.
If you select the Read-Only checkbox, users can view the contents of the hard disk but cannot modify them or save files on the hard disk.
- 8 Select options for External Disks (other than CDs or DVDs).
Select the Authentication checkbox to require a password to access external disks.
Deselect the Allow checkbox to prevent access to external disks.
If you select the Read-Only checkbox, users can view the contents of external disks but cannot modify them or save files on external disks.
- 9 Click Apply Now.

Ejecting Items Automatically When a User Logs Out

On computers used by more than one person, such as in a computer lab, users may sometimes forget to take their personal media with them when they leave. If they do not eject disks, CDs, or DVDs when they log out, these items may be available to the next user who logs in.

If you allow users to access CDs, DVDs, or external disks, such as Zip disks or FireWire drives, on shared computers, you may want to make computers eject removable media automatically when a user logs out.

To eject removable media automatically:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.

- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Media Access preference icon.
- 5 Set the management setting to Always. This setting applies to all Media Access preference options.
- 6 Click Other Media.
- 7 Select “Eject all removable media at logout.”
- 8 Click Apply Now.

Managing Printing Preferences

Use Printing preferences to create printer lists and manage access to printers.

Printer List Preferences

Printer List settings let you create a list of available printers and control the user’s ability to add additional printers or access a printer connected directly to a computer.

Making Printers Available to Users

To give users access to printers, you first need to set up a printer list. Then, you can allow specific users or groups to use printers in that list. You can also make printers available to computers. A user’s final list of printers is a combination of printers available to the user, the group selected at login, and the computer being used.

To create a printer list for users:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Printing preference icon.
- 5 Select a management setting (Once or Always). This setting applies to all Printing preference options.
- 6 Click Printer List.
- 7 The Available Printers list is created from the list of available network printers in the Print Center application.

Select a printer in the Available Printers list, then click “Add to List” to make that printer available in the User’s Printer List.

If the printer you want doesn’t appear in the Available Printers list, click Open Print Center and add the printer to Print Center’s printer list.

- 8 Click Apply Now.

Preventing Users From Modifying the Printer List

If you want to limit a user’s ability to modify a printer list, you can require an administrator’s user name and password in order to add new printers. You can also remove this privilege outright.

To restrict access to the printer list:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Printing preference icon.
- 5 Select a management setting (Once or Always). This setting applies to all Printing preference options.
- 6 Click Printer List.
- 7 If you want only administrators to modify the printer list, select “Require an administrator password.”
- 8 If don’t want any user to modify the printer list, deselect “Allow users to add printers to the Printer list.”
- 9 Click Apply Now.

Restricting Access to Printers Connected to a Computer

In some situations, you want only certain users to print to a printer connected directly to their computers. For example, if you have a computer in a classroom with a printer attached, you can reserve that printer for teachers only by making the teacher an administrator and requiring an administrator’s user name and password to access the printer.

To restrict access to a printer connected to a specific computer:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.

- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Printing preference icon.
- 5 Select a management setting (Once or Always). This setting applies to all Printing preference options.
- 6 Click Printer List.
- 7 If you want only administrators to use the printer, select “Require an administrator password.”
- 8 If don’t want any user to access the printer, deselect “Allow printers that connect directly to the user’s computer.”
- 9 Click Apply Now.

Printer Access Preferences

Access settings let you specify a default printer and restrict access to specific printers.

Setting a Default Printer

Once you have set up a printer list, you can specify one printer as the default printer. Any time a user tries to print a document, this printer is the preferred selection in an application’s printer dialog box.

To set the default printer:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Printing preference icon.
- 5 Select a management setting (Once or Always). This setting applies to all Printing preference options.
- 6 Click Access.
- 7 Select a printer in the user’s printer list, then click Make Default.
- 8 Click Apply Now.

Restricting Access to Printers

You can require an administrator’s user name and password in order to print to certain printers.

To restrict access to a specific printer:

- 1 Open Workgroup Manager.
- 2 Use the At pop-up menu to find the directory domain that contains the account you want, then click Preferences.
- 3 Click the lock and enter your user name and password.
- 4 Select a user, group, or computer account in the account list, then click the Printing preference icon.
- 5 Select a management setting (Once or Always). This setting applies to all Printing preference options.
- 6 Click Access.
- 7 Select a printer in the user's printer list, then select "Require administrator password."
- 8 Click Apply Now.

Print Service

Print service lets you share network printers for clients of the Mac OS X Server. You share printers by setting up print queues for them. 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, you can

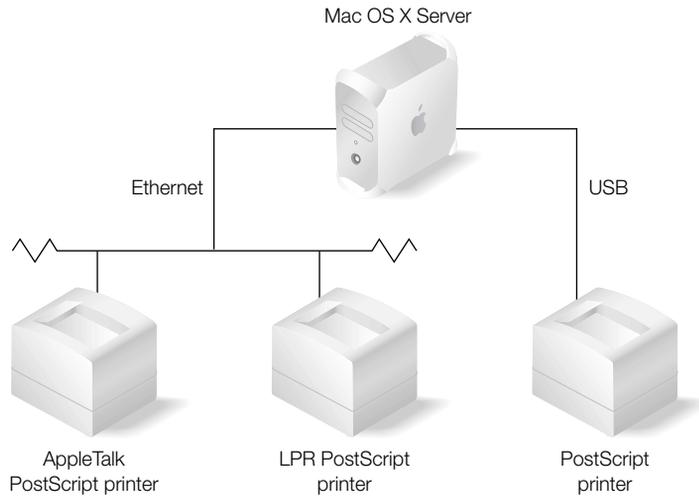
- set the priority of print jobs in a queue
- hold the printing of a job for a particular time of day
- place a job on hold indefinitely

The following applications help you administer print service:

- The Print module of Server Settings lets you configure general print service settings, set up how print queues are shared, and manage print jobs submitted to shared printers.
- Server Status lets you monitor the status of print jobs.
- The Accounts module of Workgroup Manager lets you set print quotas for users.

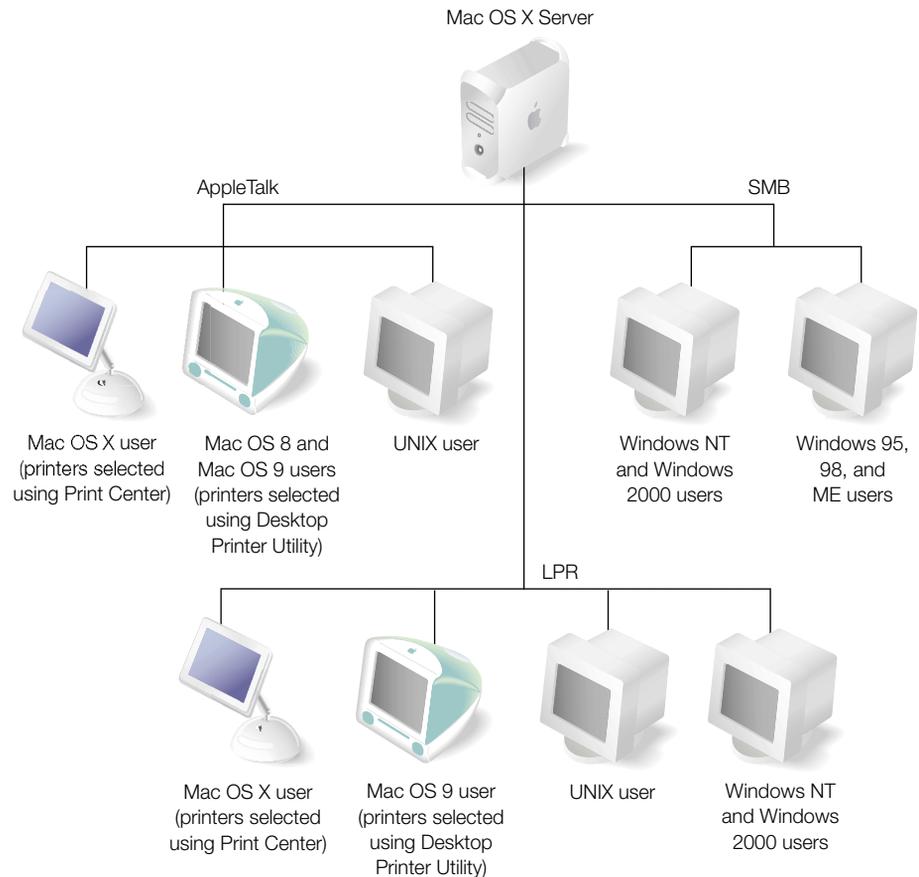
What Printers Can Be Shared?

Mac OS X Server supports PostScript-compatible printers connected to your network using AppleTalk or the Line Printer Remote (LPR) protocol. Mac OS X Server also supports PostScript-compatible printers connected directly to your server by means of a Universal Serial Bus (USB) connection.



Who Can Use Shared Printers?

Shared printers can be used over the network by users who submit print jobs using AppleTalk, LPR, or Server Message Block (SMB) protocols:



Macintosh computers support AppleTalk and LPR. Windows computers use LPR and SMB. UNIX computers use LPR. See “Setting Up Printing on Client Computers” on page 323.

Setup Overview

Here is an overview of the basic steps for setting up print service:

Step 1: Read “Before You Begin”

Read “Before You Begin” on page 319 for issues that you should consider before setting up print service.

Step 2: Start up and configure print service

Use Server Settings to start up and configure the print service. Print service configuration lets you set options that apply to all print queues that you are sharing—for example, starting print service automatically when the server starts up. See “Starting Up and Configuring Print Service” on page 319.

Step 3: Add printers and configure their print queues

You make printers available to users by adding them to the server using the Print module of Server Settings. When you add a printer, a print queue is created automatically. Users see these print queues as printers from their desktops.

You then configure the print queues, also using the Print module of Server Settings. See “Adding Printers” on page 320 and “Configuring Print Queues” on page 320.

Step 4: (Optional) Add print queues to a shared Open Directory domain

You can add print queues to a shared Open Directory domain for users of Mac OS X computers that have access to the domain. This makes it easier for Mac OS X client users to locate shared printers because these print queues show up automatically in Print Center Directory Services lists. See “Adding Print Queues to Shared Open Directory Domains” on page 321.

Step 5: (Optional) Set print quotas for users

If you want to limit the number of pages users can print, set print quotas for user accounts and enforce quotas on print queues. See “Setting Up Print Quotas” on page 322.

Step 6: Set up printing on client computers

Mac OS X clients: Add one or more print queues to users’ printer lists using Print Center.

Mac OS 9 and Mac OS 8 clients: Use the Chooser to add AppleTalk printers or use Desktop Printer Utility to add LPR printers to the clients’ desktops.

Windows clients: If you have Windows clients using SMB, you need to make sure Windows services are running and that at least one print queue is available for SMB users.

UNIX clients: Most UNIX systems support LPR. Some configuration may be required. Refer to the manufacturer’s documentation on setting up LPR printers or consult your UNIX administrator.

See “Setting Up Printing on Client Computers” on page 323.

Before You Begin

Before you set up print service, determine which protocols are used for printing by client computers. When you configure a print queue, you will need to enable each of the required protocols. Print service supports the following protocols:

- AppleTalk
- Line Printer Remote (LPR)
- Server Message Block (SMB)

See “Setting Up Printing on Client Computers” on page 323.

Security Issues

In general, AppleTalk and LPR printers do not have any provisions for security. Windows services require that users log in by providing a user name and password before using SMB printers. See “Windows User Password Validation” on page 236.

Setting Up Print Service

The following sections tell you how to configure your server’s print service, and how to create and configure print queues for the server.

Starting Up and Configuring Print Service

Use the Print module of Server Settings to start up and configure print service.

To start up and configure print service:

- 1** In Server Settings, click the File & Print tab.
- 2** Click Print and choose Start Print Service.
- 3** Click Print again and choose Configure Print Service.
- 4** Select “Start print service at system startup” if you want print service to start automatically when the server starts up.
- 5** Select “Automatically share new queues for Windows printing” 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, make sure that Windows services are running. See “Starting Windows Services” on page 240.

- 6** Choose the default queue for LPR print jobs.

Using a default queue simplifies the setup for printing from client computers. See “Selecting a Default Print Queue” on page 329.

If you choose None, print jobs sent to the default queue will not be accepted by the server (and therefore will not be printed).

- 7 Select “Server log” if you want to archive the print service log file. Specify how often (by entering the number of days) you want to archive the current log and start a new one.
- 8 Select “Queue logs” if you want to archive the print queues’ log files. Specify how often (by entering the number of days) you want to archive the current log and start a new one.

Adding Printers

You can share any PostScript-compatible printer that has a queue defined for it on the server. You use the Print module of Server Settings to “add” printers to the server. When you add a printer, the print queue is created automatically.

Note: You do not need to “add” USB printers connected directly to the server. Queues for USB printers are created automatically without that step.

To add a printer and create a print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Click New Queue.
- 4 Choose the protocol used by the printer you want to add from the pop-up menu.
- 5 For “AppleTalk” or “Directory Services” printers, select a printer in the list and click Add. For “LPR Printers using IP,” enter the printer Internet address or DNS name, select whether to use the default queue on the server, enter the queue name, and click Add.

If you want to print from the server, set up a print queue on the server using Print Center.

Configuring Print Queues

You configure a print queue to specify which protocols to use to share the queue and to specify the default settings for new print jobs. You can also change the name of the queue.

To configure a print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the print queue you want to configure and click Edit.
- 4 If you want users to see a name other than the Print Center queue name, enter 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.

Queue names shared via LPR or SMB should not contain characters other than A–Z, a–z, 0–9, and “_” (underscore).

AppleTalk queue names cannot be longer than 32 bytes (which may be fewer than 32 typed characters). Note that the queue name is encoded according to the language used on the server and may not be readable on client computers using another language.

- 5 Select the protocols used for printing by your client computers.

If you select “Windows printing (SMB),” make sure Windows services are running.

See “Starting Windows Services” on page 240.

- 6 If you want to add the queue to a shared Open Directory domain, choose a 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.

This allows users of Mac OS X computers configured to access the domain to print to the queue by choosing it from the Directory Services printer list in Print Center (rather than having to manually enter the LPR print host and queue name).

Note: After sharing a print queue in an Open Directory domain, do *not* try to add the queue from the Directory Services list to your server.

- 7 Choose the default job priority for new print jobs in this queue.
- 8 Select Hold to postpone printing all new jobs that arrive in the queue. Specify a time of day to print the jobs, or choose to postpone printing indefinitely.
- 9 Select “Enforce print quotas” if you want to enforce the user print quotas for the printer.

Adding Print Queues to Shared Open Directory Domains

If you add a print queue to a shared Open Directory domain, users of Mac OS X computers that are configured to access the domain can print to the queue by choosing it from the Directory Services printer list in Print Center (rather than having to manually enter the LPR print host and screen name).

To add a print queue to a shared Open Directory domain:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue you want to add and click Edit.
- 4 Choose a shared domain from the “Share LPR Queue in Domain” pop-up menu. Enter the user name and password for the administrator of the server on which the domain resides.

The Open Directory printer is named using the queue name defined in the Print module of Server Settings.

LPR clients do not support names that contain spaces, and some Windows clients restrict names to 12 characters. Queue names shared via LPR or SMB should not contain characters other than A–Z, a–z, 0–9, and “_” (underscore).

AppleTalk queue names cannot be longer than 32 bytes (which may be fewer than 32 typed characters). Note that the queue name is encoded according to the language used on the server and may not be readable on client computers using another language.

Note: After sharing a print queue in an Open Directory domain, do *not* try to add the queue from the Directory Services list to your server.

Setting Up Print Quotas

There are two parts to setting up print quotas—specifying the quotas in users’ accounts and enforcing the quotas for the print service. You use the Users & Groups module of Workgroup Manager to set up print quotas for a user. You can set specific quotas for each print queue or you can define a single quota that applies to all print queues (that are enforcing quotas) to which a user has access. See “Working With Print Settings for Users” on page 151.

You use Server Settings to “turn on” the enforcement of users’ print quotas that you’ve defined for a print queue. If you do not enforce print quotas, users can print an unlimited number of pages to the queue.

Enforcing Quotas for a Print Queue

Unless you enforce quotas for a print queue, users will have unlimited printing capabilities even if print quotas are defined for the users’ accounts.

To enforce quotas for a print queue:

- 1** In Server Settings, click the File & Print tab.
- 2** Click Print and choose Show Print Monitor.
- 3** Select the print queue and click Edit.
- 4** Select “Enforce print quotas” to enforce the user print quotas for the print queue.

Setting Up Printing on Client Computers

Mac OS X Clients

Mac OS X users must add shared print queues to their Print Center printer lists before they can use the queues. Mac OS X supports both AppleTalk and LPR printers. Users can also add print queues in Open Directory domains accessible from the Mac OS X computer.

If a Mac OS X client is having trouble printing, see “Solving Problems” on page 334.

Adding a Print Queue in Mac OS X Using AppleTalk

You use the Print Center to add print queues to a computer’s printer lists. Print Center is usually located in the Utilities folder of the Applications folder.

To add a print queue using AppleTalk:

- 1 Open the Print Center and click Add Printer.
- 2 Choose AppleTalk from the pop-up menu.
- 3 Select a printer from the list and click Add.

Adding a Print Queue in Mac OS X Using LPR

You use the Print Center to add print queues to a computer’s printer lists. Print Center is usually located in the Utilities folder of the Applications folder.

To add a print queue using LPR:

- 1 Open the Print Center and click Add Printer.
- 2 Choose “LPR Printers using IP” from the pop-up menu.
- 3 Enter the server’s DNS name or IP address in the LPR Printer’s Address field.

To use the default queue, select the “Use Default Queue on Server” option.

If the server does not have a default LPR queue defined or you do not want to use the default queue, remove the checkmark and enter a queue name in the Queue Name field.

- 4 Choose a description of the printer from the Printer Model pop-up menu, then click Add.

Adding a Print Queue From an Open Directory Domain

You use the Print Center to add print queues to a computer’s printer lists. Print Center is usually located in the Utilities folder of the Applications folder.

To add a print queue from an Open Directory domain:

- 1 Open the Print Center and click Add Printer.
- 2 Choose Directory Services from the pop-up menu.
- 3 Select a queue, then click Add.

Mac OS 8 and Mac OS 9 Clients

Mac OS 8 and 9 support both AppleTalk and LPR printers. Users can set up printing to a server print queue by using the Chooser for AppleTalk printers or Desktop Printer Utility for LPR printers. (The Desktop Printer Utility is usually located in the LaserWriter Software folder in the Apple Extras folder or in the Utilities folder in the Applications folder.)

If a Mac OS 8 or 9 client is having trouble printing, see “Solving Problems” on page 334.

Setting Up Printing on Mac OS 8 or 9 Client for an AppleTalk Printer

You use the Chooser to set up AppleTalk printers.

To set up printing for an AppleTalk printer:

- 1 Open the Chooser.
- 2 Select the LaserWriter 8 icon or the icon for your printer’s model.

The LaserWriter 8 icon works well in most cases. Use a printer-specific icon, if available, to take advantage of special features that might be offered by that printer.

- 3 Select the print queue from the list on the right.
- 4 Close the Chooser.

Setting Up Printing on Mac OS 8 or 9 Clients for an LPR Printer

You use the Desktop Printer Utility to set up LPR printers.

To set up printing for an LPR printer:

- 1 Open the Desktop Printer Utility and select Printer (LPR). Click OK.
- 2 In the PostScript printer Description (PPD) File section, click Change and select the PPD file for the printer. Choose Generic if you do not know the printer type.
- 3 In the LPR Printer Selection section, click Change and enter the server’s IP address or domain name in the Printer Address field.
- 4 Enter the name of a print queue on the server that is configured for sharing via LPR. Leave the field blank if you want to print to the default LPR queue.
- 5 Click Verify to confirm that print service is accepting jobs via LPR.
- 6 Click OK, then Create.
- 7 Enter a name and location for the desktop printer icon, and click Save.

The default name is the printer’s IP address, and the default location is the Desktop.

Windows Clients

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 “Starting Windows Services” on page 240 and “Adding Printers” on page 320.

All Windows computers—including Windows 95, Windows 98, Windows Millennium Edition (ME), and Windows XP—support SMB for using printers on the network. Windows 2000 and Windows NT also support LPR.

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

If a Windows client is having trouble printing, see “Solving Problems” on page 334.

UNIX Clients

UNIX computers support LPR for connecting to networked printers without the installation of additional software.

If a UNIX client is having trouble printing, see “Solving Problems” on page 334.

Managing Print Service

This section tells you how to perform day-to-day management tasks for print service once you have it up and running.

Monitoring Print Service

Server Status lets you monitor all services on a Mac OS X server.

If you want to make changes to print service, use Server Settings.

To monitor print service:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select Print in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Overview tab to see if print service is running, the time it started if it is running, and the number of queues.
- 3 Click the Logs tab to see print service logs for the system and for individual print queues.
Use the Show pop-up menu to choose which log to view.
- 4 Click Queues to see the status of print queues.

The table includes the name of the printer, type of print queue, number of jobs, sharing, and status for each queue.

Stopping Print Service

You use the File & Print pane in Server Settings to stop print service.

To stop print service:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Stop Print Service.

Setting Print Service to Start Automatically

You can set print service to start automatically when the server starts up.

To start print service automatically when the server starts up:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Configure Print Service.
- 3 Select “Start Print Service at system startup.”

Managing Print Queues

This section tells you how to perform day-to-day management of print queues.

Monitoring a Print Queue

Server Status lets you monitor all services on a Mac OS X server. The Queues pane lists the queues for the print service and tells you the name or kind of printer, how many jobs are pending, how the printer is shared, whether a job is printing, and, if so, the status of that job.

If you want to make changes to a print queue, use Server Settings.

To monitor a print queue:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select Print in the list of services under the server name.

If the services aren't visible, click the arrow to the left of the server name.

- 2 Click the Queues tab to see the status of the print queues.

The table includes the name of the printer, type of print queue, number of jobs, sharing, and status for each queue.

Putting a Print Queue on Hold (Stopping a Print Queue)

To prevent jobs in a queue from printing, put the print queue on hold. Printing of all jobs waiting to print is postponed. New jobs are still accepted but won't be printed until the queue is started up again and the jobs ahead of it (of the same or higher priority) are printed. If a job is printing, it is canceled and reprinted from the beginning when the queue is restarted.

To put a print queue on hold:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the print queue you want to hold and click Hold.

Restarting a Print Queue

If you put a print queue on hold, restart the print queue to resume printing for all jobs that have not been put on hold individually.

If a job was in the middle of printing when you put the print queue on hold, that job will be printed again from the beginning.

To restart a print queue that's been put on hold:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue and click Release in the Print Monitor window.

Changing a Print Queue's Configuration

Use the Server Settings Print Monitor to view and change a print queue's configuration.

Note: When you change a print queue's configuration, the queue may become unavailable to users. You may need to alert users to set up client computers to use the queue again.

To change a print queue's configuration:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print, and choose Show Print Monitor.
- 3 Select the print queue you want to change and click Edit.
- 4 If you want users to see a name other than the Print Center queue name, enter 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.

Note: If you change the name of a print queue that has already been shared, print jobs sent by users to the old queue name will not be printed. Users will need to set up their computers again to use the queue with its new name.

- 5 Select the protocols used for printing by your client computers.

If you select “Windows printing (SMB),” make sure Windows services are running.

See “Starting Windows Services” on page 240.

- 6 If you want to add the queue to a shared Open Directory domain, choose a 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.

This allows users of Mac OS X computers configured to access the domain to print to the queue by choosing it from the Directory Services printer list in Print Center (rather than having to manually enter the LPR print host and queue name).

Note: After sharing a print queue in an Open Directory domain, do *not* try to add the queue from the Directory Services list to your server.

- 7 Choose the default job priority for new print jobs in this queue.
- 8 Select Hold to postpone printing all new jobs that arrive in the queue. Specify a time of day to print the jobs, or choose to postpone printing indefinitely.
- 9 Select “Enforce print quotas” if you want to enforce the user print quotas for the printer.

Renaming a Print Queue

When you add a printer in Print Center, the default name of the queue created for it is the same as the printer name.

Note: If you change the name of a print queue that has already been shared, print jobs sent by users to the old queue name will not be printed. Users will need to set up their computers again to use the queue with its new name.

To rename a print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the print queue you want to rename and click Edit.
- 4 Enter a new name in the Queue Name field.

Entering a queue name does not change the Print Center queue name.

Selecting a Default Print Queue

Specifying a default print queue simplifies setup for printing from client computers to LPR print queues. Users can choose to print to the default queue rather than having to enter the IP address of a specific queue.

To select a default print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Configure Print Service.
- 3 Choose the queue you want to make the default queue from the “Default Queue for LPR” pop-up menu.

Deleting a Print Queue

When you delete a print queue, any jobs in the queue that are waiting to print are also deleted.

Note: If a job is printing, it is canceled immediately. To avoid abruptly canceling users’ print jobs, you can turn off sharing a queue until all jobs have finished printing and then delete the queue.

To delete a print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the print queue you want to delete and click Delete.

Managing Print Jobs

This section tells you how to perform day-to-day management of print jobs.

Monitoring a Print Job

You monitor individual print jobs using the Queue Monitor window of Server Settings.

To monitor a print job:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue and click Show Queue Monitor.

The Queue Monitor window displays all the current print jobs in priority order. It also indicates the current status of the active (printing) job, the name of the user who submitted each job, and the number of pages and sheets in each job. The number of pages is the number of pages in the document. The number of sheets is the physical number of pages in the queue, which reflects the number of copies or the number of pages printed on one sheet of paper. For example, a Page/Sheets value of 4/20 appears if a user prints five copies of a four-page document.

Stopping a Print Job

You can stop a job from printing by putting it or the queue in which it resides on hold.

To put a single print job on hold, see the following section. To put a print queue on hold to stop jobs from printing, see “Putting a Print Queue on Hold (Stopping a Print Queue)” on page 327.

Putting a Print Job on Hold

When you put a print job on hold, it is not printed until you take it off hold or until the date and time you set it to be printed has been reached. If the job has already started to print, printing stops and the job remains in the queue. When you take the job off hold, printing starts from the beginning of the job.

Use Shift-click or Command-click to select multiple jobs and put them all on hold at the same time.

To put a print job on hold:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue containing the job, then click Show Queue Monitor.
- 4 Select the job and click Hold.
- 5 If you want to take the job off hold automatically at a certain time, click Set Priority, then specify the date and time to release the job for printing.

If there are other jobs of equal or higher priority in the print queue when the print job is released, the actual print time will be later.

Restarting a Print Job

When a print job has been placed on hold, it is not printed until you restart the job or until the time you set it to be printed has been reached.

Note: If you put the print queue on hold, restart the print queue to print the job.

To restart a print job:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue containing the job, then click Show Queue Monitor.
- 4 Select the job and click Release.

The job is returned to the print queue and is printed after all other jobs in the queue with the same priority.

Holding All New Print Jobs

You can automatically postpone printing all new jobs that arrive in a print queue.

To hold new print jobs:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue and click Edit.
- 4 Select the Hold checkbox. Choose Until to specify a time of day at which to print new jobs. Choose Indefinitely to postpone printing new jobs indefinitely.

Setting the Default Priority for New Print Jobs

When a new print job is sent to a print queue, it is assigned the priority defined for the print queue. Jobs are printed in order of priority. Urgent jobs are printed first, then Normal jobs, and finally Low jobs.

To set the default priority for new print jobs in a queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue and click Edit.
- 4 Under the “Default Settings for New Jobs” section, choose a job priority of Urgent, Normal, or Low.

Changing a Print Job’s Priority

When a print job arrives in a queue, it is assigned the default priority for that queue. You can override the default by changing the priority for the individual print job.

To change a print job’s priority:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.

- 3 Select the queue containing the job, then click Show Queue Monitor.
- 4 Select the job and click Set Priority.
- 5 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 other job in the queue with the same priority.

Deleting a Print Job

If a job is printing at the time you delete it, the job will stop printing after the pages in the printer's hardware buffer have been printed.

To delete a print job:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Show Print Monitor.
- 3 Select the queue containing the job, then click Show Queue Monitor.
- 4 Select the job and click Delete.

Managing Print Quotas

This section tells you how to perform day-to-day management of print quotas.

Suspending Quotas for a Print Queue

You use the Print module of Server Settings to enforce and suspend print quotas. Suspending quotas for a print queue allows all users unlimited printing to the queue.

To enforce or suspend quotas for a print queue:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Configure Print Service.
- 3 Select the print queue and click Edit.
- 4 Deselect the "Enforce print quotas" option.

To enforce print quotas again, select the "Enforce print quotas" option again.

Managing Print Logs

This section tells you how to view and archive print logs.

Viewing Print Logs

Print service has two kinds of logs: print service and print queue. Print service logs record 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.

You can view the print service logs using Server Status.

To view print service logs using Server Status:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select Print in the list of services under the server name. If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Logs tab to see print service logs for the system and for individual print queues. Use the Show pop-up menu to choose which log to view.

Archiving Print Logs

As noted, print service maintains two kinds of logs: a print service log and a log for each print queue. You can specify how often you want to archive the logs and start new ones. All logs, both current and archived, are kept in the `/Library/Logs/PrintService` folder. Archived files are kept until they are manually deleted by the server administrator.

To specify how often to archive print logs:

- 1 In Server Settings, click the File & Print tab.
- 2 Click Print and choose Configure Print Service.
- 3 Select “Server log” and enter a number of days to specify how often you want to archive the print service log and start a new log.

The current log file name is `PrintService.server.log`. Archived print service log files have the archive date appended (for example, `PrintService.server.log.20021231`).

- 4 Select “Queue logs” and enter a number of days to specify how often you want to archive each print queue log and start a new one.

The log files are stored in `/Library/Logs/PrintService`. Individual log files are named after the print queues (for example, `PrintService.myqueue.job.log`). Archived print queue log files have the archive date appended (for example, `PrintService.myqueue.job.log.20021231`).

You can view current log files using Server Status.

You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See “Log Rolling Scripts” on page 555.

Deleting Print Log Archives

The log files are stored in `/Library/Logs/PrintService`. You can clear out unwanted archive files by deleting them from this directory using the Finder.

You can also use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files. See “Log Rolling Scripts” on page 555.

Solving Problems

Try these suggestions to solve or avoid printing problems.

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” option 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 Change Product Serial Number.
- Use Server Status to review the print service log for additional information.

Users Can't Print

- Check to see that print service is running. Open Server Settings and select the File & Print tab. If the print service is not running, select Print and choose Start Print Service.
- 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 Chooser (for AppleTalk print queues) or Desktop Printer Utility (for LPR print queues) to make sure the printer setup is correct. On Mac OS X, use the Print Center to add print queues to the printer list.
- 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 on Macintosh, UNIX, and other computers, can use for printing.
- Verify that Mac OS 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.

Print Jobs Don't Print

- Check the Print Monitor window to make sure that the queue is not on hold. Open Server Settings, click the File & Print tab, click Print, and choose Show Print Monitor.
- Make sure 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. Open Server Status, select Print under the server name in the Devices & Services list, and click the Logs tab.

Print Queue Becomes Unavailable

- If you changed a print queue's name that has already been shared, print jobs sent by users to the old queue name will not be printed. Users need to set up their computers again to use the queue with its new name.

See "Setting Up Printing on Client Computers" on page 323.

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. A Web server responds to requests for HTML Web pages stored on your site. Open-source software allows anyone to view and modify the source code to make changes and improvements. This has led to Apache's widespread use, making it the most popular Web server on the Internet today.

Web administrators can use Server Settings 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, and then check the pages 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.

Since Web service is based on Apache, you can add advanced features with plug-in modules. Apache modules allow you to add support for Simple Object Access Protocol (SOAP), Java, and CGI languages such as Python.

Before You Begin

This section provides information you 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 Settings 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 Settings, 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 361.

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
- verify that DNS is properly configured if you want clients to access your Web site by name

When you are ready to publish, or enable, your site, you can do this using Server Settings. 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. See “Managing Web Sites” on page 349 for more information.

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 share the same domain name, IP address, or port. The unique combination of domain name, IP address, and port identifies each separate 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. This is an issue only with software released prior to 1997 and does not affect modern browsers. If you think your users will be using very old browser software, you'll need to configure your sites with one domain name per IP address.

Understanding WebDAV

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 "Setting Access for WebDAV-Enabled Sites" on page 354.

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 user named "www" and a group named "www" in the server's Users & Groups List. The Apache processes that serve Web pages run as the www user and as members of the www group. You need to give the www group read access to files within Web sites so that the server can transfer the files to browsers when users connect to the sites. If you're using WebDAV, the www user and www group both need write access to the files and folders in the Web sites. In addition, the www user and group need write access to the /var/run/davlocks directory.

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 Settings. Mac OS X Server uses a predefined group named “www,” which contains the Apache processes. You need to give the www group read and write access to files within the Web site. You also need to assign read and write access to the Web site administrator (owner) and None (no access) 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.

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
- php for “PHP: Hypertext Preprocessor” (embedded HTML scripts) used for WebMail, etc.
- tiff for TIFF (graphics) files

Mac OS X Server includes a default set of MIME type suffixes. This set includes all the suffixes in the mime.types file distributed with Apache, with a few additions. If a suffix you need is not listed, or does not have the behavior you want, use Server Settings to add the suffix to the set or to change its behavior.

Note: Do not add or change MIME suffixes by editing configuration files.

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 and 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.

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 “Managing Web Service” on page 342 and “Managing Web Sites” on page 349.

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 in the user’s Sites folder will be served from this URL:

```
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 “Managing Web Sites” on page 349.

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 creates a group named "www," made up of the Apache processes. 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, but you can configure all the basic features of Web service and Web sites using Server Settings.

To host user Web sites, you must configure at least one Web site. 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 "Managing Web Service" on page 342.

Step 5: Start Web service

In Server Settings, click the Internet tab. Click Web and choose Start Web Service.

When the service is running, you see a globe on the Web icon.

Important Always use Server Settings to start and stop the Web server. You can start the Web server from the command line, but Server Settings won't show the change in status for several seconds. Server Settings is the preferred method to start, stop, and modify Web service settings.

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" on page 364.

Managing Web Service

The Configure Web Service window lets you set and modify most options for your Web service and Web sites.

To access the Configure Web Service window:

- 1 In Server Settings, click Web and choose Configure Web Service.
- 2 Click one of the four tabs to see the settings in that pane.

Starting or Stopping Web Service

You start and stop Web service from the Server Settings application.

To start or stop Web service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Start Web Service or Stop Web Service.

If you stop Web service, users connected to any Web site hosted on your server are disconnected immediately.

Important Always use Server Settings to start and stop the Web server. You can start the Web server from the command line, but Server Settings won't show the change in status for several seconds. Server Settings is the preferred method to start, stop, and modify Web service settings.

Starting Web Service Automatically

You can set Web service to start automatically whenever the server starts up. This will ensure that your Web sites are available if there's been a power failure or the server shuts down for any reason.

To have Web service start automatically:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Select "Start Web service on system startup."

Modifying MIME Mappings

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 340.

The Web server is set up to handle the most common MIME types. You can add, edit, or delete MIME type mappings.

To add or modify a MIME type mapping:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the MIME Types tab.
- 4 Click Add to add a new mapping, or select a mapping and click Edit, Duplicate, or Delete. (If you choose Delete, you've finished.)

- 5 Type the file suffix that describes the type of data in files handled by this mapping.
- 6 Choose a Web server response from the Response pop-up menu. If you choose “Return file as MIME type,” enter the MIME type you want to return.
- 7 Click Save.

If you choose a response that is a Common Gateway Interface (CGI) script, make sure you have enabled CGI execution for your site in the Options pane of the site settings window.

Setting Up Persistent Connections for Web Service

You can set up Web service to respond to multiple requests from a client computer without closing the connection each time. Repeatedly opening and closing connections isn't very efficient and decreases performance.

To set up persistent connections:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 In the General pane, enter a number in the Maximum Persistent Connections field.
If you set the number to zero, there is no limit to the number of requests allowed per connection. However, the default setting of 500 provides better performance.
- 4 Enter a number in the Connection Timeout field if you want to specify the amount of time that can pass between requests before the session is disconnected by the Web server.
- 5 Click Save, then restart Web service.

Limiting Simultaneous Connections for Web Service

You can limit the number of simultaneous connections to your Web server. When the maximum number of connections is reached, new requests receive a message that the server is busy.

To set the maximum number of connections to your Web server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 In the General pane, enter a number in the Maximum Simultaneous Requests field.
The default maximum is 500, but you can set the number as high or as low as you want to, taking into consideration the desired performance of your server.
- 4 Click Save, then restart Web service.

Setting Up Proxy Caching for Web Service

A proxy lets users check a local server for frequently used files. You can use a proxy to speed up response times and reduce network traffic. The proxy stores recently accessed files in a cache on your Web server. Browsers on your network check the cache before retrieving files from more distant servers.

To take advantage of this feature, client computers must specify your Web server as their proxy server in their browser preferences.

To set up a proxy:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Proxy tab and select Enable Proxy.
- 4 Set the maximum cache size.

When the cache reaches this size, the oldest files are deleted from the cache folder.

- 5 Type the path name for the folder in the Cache Folder field.

You can also click the Select button and browse for the folder you want to use.

If you are administering a remote server, file service must be running on the local machine to use the Select button.

If you change the folder location from the default, you will have to select the new folder in the Finder, select Get Info and change the owner and group to www.

- 6 Click Save, then restart Web service.

Blocking Web Sites From Your Web Server Cache

If your Web server is set up to act as a proxy, you can prevent the server from caching objectionable Web sites.

Important To take advantage of this feature, client computers must specify your Web server as their proxy server in their browser preferences.

You can import a list of Web sites you want to block. The list must be a text file with the host names separated by white space (lines, spaces, or tabs).

To block Web sites:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Proxy tab and select Enable Proxy.

- 4 Type the URL of the Web site you want to block in the field and click Add. Or click Import to import a list of Web sites.
- 5 Click Save, then restart Web service.

Enabling SSL for Web Service

If you plan to set up Secure Sockets Layer (SSL) service and enable it for Web sites, you need to enable it for the entire Web service. Once you enable SSL service you can configure SSL for each site hosted on your server.

For more information about configuring SSL for a specific Web site, see “Enabling SSL” on page 357.

To enable SSL for Web service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click “Enable SSL support.”
- 4 Click Save, then restart Web service.

Setting Up the SSL Log for a Web Server

If you are using Secure Sockets Layer (SSL) on your Web server, you can set up a file to log SSL transactions and errors.

To set up an SSL log:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab, select a site to edit, then click Edit.
- 4 Click the Security tab, select Enable Secure Sockets Layer (SSL), then enter the path name for the folder where you want to keep the SSL log in the SSL Log File field.
- 5 Click Save, then restart Web service.

Setting Up WebDAV for a Web Server

Web-based Distributed Authoring and Versioning (WebDAV) allows you or your users to make changes to Web sites while the sites are running. If you enable WebDAV, you also need to assign access privileges for the sites and for the Web folders.

To enable WebDAV:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.

- 3 In the General pane, select “Enable WebDAV support,” then click the Sites tab.
- 4 Select a Web site and click Edit, click the Options tab, then select Enable WebDAV.
- 5 Click the Access tab. Select a realm and click Edit, or click Add to create a new realm.
The realm is the part of the Web site users can access.
- 6 Type the name you want users to see when they log in.
The default realm name is the name of the Web site.
- 7 Type the path to the location in the Web site to which you want to limit access.
You can also click the Select button and browse for the folder you want to use.
If you are administering a remote server, file service must be running on the local machine to use the Select button.
- 8 Click Save.

Starting Tomcat

Tomcat adds Java servlet and JavaServer Pages (JSP) capabilities to Mac OS X Server. Java servlets are Java-based applications that run on your server, in contrast to Java applets which run on the user’s computer. JavaServer Pages allows you to embed Java servlets in your HTML pages.

For more information on Tomcat see “Installing and Viewing Web Modules” on page 365.

You can set Tomcat to start automatically whenever the server starts up. This will ensure that the Tomcat module starts up after a power failure or after the server shuts down for any reason.

Note: Tomcat is not started by a Startup Item, nor is it started directly by the watchdog process. It is started and stopped by the Server Settings application in conjunction with the `serversettingsd` process, which uses the `/Library/Tomcat/bin/tomcatctl` script.

To start Tomcat on server startup:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click “Start Tomcat at system startup.”
- 4 Click Save, then restart the server.

To verify that Tomcat is running, use a Web browser to access port 9006 of your Web site by entering the URL for your site followed by `:9006` (see the URL below).

`http://example.com:9006`

If Tomcat is running, accessing port 9006 will display the default Tomcat home page.

Checking Web Service Status

In the Server Settings application, you can check to see the current state of the server and the performance cache, and which Web modules are active. The Start/Stop Status Messages field displays messages about the server status. If you are not sure what the messages mean, you can find explanations on the Apache Web site:

www.apache.org

If Web service is not running, the window shows only the date and time the server stopped.

To view Web service status:

- 1 In Server Settings, click Internet.
- 2 Click Web and select Show Web Service Status.

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

Performance cache requests and throughput include performance cache data only.

Viewing Logs of Web Service Activity

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.

To view the log files:

- 1 In Server Status, click Web under your server.
- 2 Click the Logs tab.
- 3 Click the log you want to view.

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, and then use the Web module of Server Settings 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.

Managing Web Sites

The Sites pane lists your Web sites and provides some basic information about each site. You use the Sites pane to add new sites or change settings for existing sites.

To access the Sites pane:

- In Server Settings, click Web and choose Configure Web Service, then click the Sites tab.

Setting Up the Documents Folder for Your Web Site

To make files available through a Web site, you put the files in the Documents folder for the site. To organize the information, you can create folders inside the Documents folder. 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/
```

To set up the Documents folder for your Web site:

- 1 Open the Documents folder on your Web server.
If you have not changed the location of the Documents folder, it's in this directory:

```
/Library/WebServer/Documents/
```
- 2 Replace the index.html file with the main page for your Web site.
Make sure the name of your main page matches the default document name you set in the General pane of the site settings window.
- 3 Copy files you want to be available on your Web site to the Documents folder.

Changing the Default Web Folder for a Site

A site's default Web folder is used as the root for the site. In other words, the default folder is the top level of the directory structure for the site.

To change the default Web folder for a site hosted on your server:

- 1 Log in to the server you want to administer.

- 2 Drag the contents of your previous Web folder to your new Web folder.
- 3 In Server Settings, log in to the server where the Web site is located.
- 4 Click the Internet tab, then click Web and choose Configure Web Service.
- 5 Click the Sites tab.
- 6 Select a site in the list, then click Edit.
- 7 Type the path to the Web folder in the Website Folder field, or click the Select button and navigate to the new Web folder location (if accessing this server remotely, file service must be turned on to do this; see Chapter 5, “File Services,” for more information).
- 8 Click Save, then restart Web service.

Enabling a Web Site on a Server

Before you can enable a Web site, you must create the content for the site and set up your site folders.

To enable the Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab, then click Add.
- 4 Type the fully qualified DNS name of your Web site in the Name field.
- 5 Enter the IP address and port number (any number up to 8999) for the site.

The default port number is 80. Make sure that the number you choose is not already in use by another service on the server.

Important In order to enable your Web site on the server, the Web site must have a unique IP address and port number combination. See “Hosting More Than One Web Site” on page 339 and “Setting Up Multiple IP Addresses for a Port” on page 348 for more information.

- 6 Enter the path to the folder you set up for this Web site.

You can also click the Select button and browse for the folder you want to use.

If you are administering a remote server, file service must be running on the local machine to use the Select button.

- 7 Enter the file name of your default document (the first page users see when they access your site).
- 8 Make any other settings you want for this site, then click Save.
- 9 Click the Enabled box next to the site name in the Sites pane of the Configure Web Service window.

- 10 Click Save, then restart Web service.

Setting the Default Page for a Web Site

The default page appears when a user connects to your Web site by specifying a directory or host name instead of a file name.

To set the default Web page:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site in the list, then click Edit.
- 5 In the General pane, type a name in the Default Document Name field.

A file with this name must be in the Web site folder.

- 6 Click Save, then restart Web service.

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

Changing the Access Port for a Web Site

By default, the server uses port 80 for connections to Web sites on your server. You may need to change the port used for an individual Web site, for instance, if you want to set up a streaming server on port 80. Make sure that the number you choose does not conflict with ports already being used on the server (for FTP, Apple file service, SMTP, and others). If you change the port number for a Web site you must change all URLs that point to the Web server to include the new port number you choose.

To set the port for a Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site, then click Edit.
- 5 Type the port number in the Port field, then click Save.

Improving Performance of Static Web Sites

If your Web sites contain static HTML files, and you expect high usage of the pages, you can enable the performance cache to improve server performance.

You should disable the performance cache if

- you do not anticipate heavy usage of your Web site
- most of the pages on your Web site are generated dynamically

The performance cache is enabled by default.

To enable or disable the performance cache for your Web server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site in the list, then click Edit.
- 5 In the Options pane, select or deselect “Enable performance cache.”
- 6 Click Save, then restart Web service.

You can also improve server performance by disabling the access and error logs.

Enabling Access and Error Logs for a Web Site

You can set up error and access logs for individual Web sites that you host on your server. However, enabling the logs can slow server performance.

To enable access and error logs for a Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site in the list, then click Edit.
- 5 Click the Logging tab and select the logs you want to enable.
- 6 Set how often you want the logs to be archived.
- 7 Type the path to the file where you want to store the logs.

You can also click the Select button and browse for the folder you want to use.

If you are administering a remote server, file service must be running on the local machine to use the Select button.

- 8 Click Save, then restart Web service.

Setting Up Directory Listing for a Web Site

When users specify the URL for a directory, you can display either a default Web page (such as index.html) or a list of the directory contents. You can display either a simple list or a detailed folder list. To set up directory listing, you need to enable indexing for the Web site.

Note: Folder listings are displayed only if no default document is found.

To enable indexing for a Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site, then click Edit.
- 5 Select “Enable indexing of folders” in the Options pane.
If you want a simple list, skip to step 8. If you want a detailed folder list, continue with the next step.
- 6 Click Save, then click the General tab of the Configure Web Service window.
- 7 Select “Enable detailed folder listings.”
- 8 Click Save, then restart Web service.

Connecting to Your Web Site

Once you configure your Web site, it’s a good idea to view the site with a Web browser to verify that everything appears as intended.

To make sure a Web site is working properly:

- 1 Open a Web browser and type the Web address of your server.
You can use either the IP address or the DNS name of the server.
- 2 Type the port number, if you are not using the default port.
- 3 If you’ve restricted access to specific users, enter a valid user name and password.

Enabling WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) allows you or your users to make changes to Web sites while the sites are running. If you enable WebDAV, you also need to assign access privileges for the sites and for the Web folders.

To enable WebDAV:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 In the General pane, select “Enable WebDAV support,” then click the Sites tab.
- 4 Select a Web site and click Edit, click the Options tab, then select Enable WebDAV.
- 5 Click the Access tab. Select a realm and click Edit, or click Add to create a new realm.
The realm is the part of the Web site users can access.
- 6 Type the name you want users to see when they log in.

The default realm name is the name of the Web site.

- 7 Type the path to the location in the Web site to which you want to limit access.

If file service is running, or if you are using Server Settings on the Mac OS X server, you can click Select and browse to find the location.

- 8 Click Save.

Setting Access for WebDAV-Enabled Sites

You create realms to provide security for Web sites. *Realms* are locations within a site that users can view or make changes to when WebDAV is enabled. When you define a realm, you can assign browsing and authoring privileges to users for the realm.

To add users and groups to a realm:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service, then click the Sites tab.
- 3 Select a site name and click Edit, then click the Access tab.
- 4 Select a realm and click Edit, or click Add to create a new realm.

The default name for a new realm is the name of the Web site.

- 5 Select the “Everyone” checkbox and choose “can Browse” from the pop-up menu.
- 6 Drag users and groups from the list of users and groups in Workgroup Manager to the realm window.
- 7 Select Allow Authoring if you want a user or group to be able to author.

If you don't select Everyone, you can fully restrict access and add only the users you want to browse and author for this realm. When you select privileges for Everyone, you have these options:

“Browse” allows everyone who can access this realm to see it. You can add additional users and groups to the User or Group list to enable authoring for them.

“Browse and Author” allows everyone who has access to this realm to see and make changes to it.

Enabling a Common Gateway Interface (CGI) script

Common Gateway Interface (CGI) scripts (or programs) send information back and forth between your Web site and applications that provide different services for the site.

- If a CGI is to be used by only one site, install the CGI in the Documents folder for the site. The CGI name must end with the suffix “.cgi.”

- If a CGI is to be used by all sites, install it in the /Library/WebServer/CGI-Executables folder. In this case, clients must include /cgi-bin/ in the URL for the site. For example, `http://www.example.com/cgi-bin/test-cgi`
- Make sure the file permissions on the CGI allow it to be executed by the user named “www.” Since the CGI typically isn’t owned by www, the file should be executable by everyone.

To enable a CGI for a Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a Web site in the list and click Edit.
- 5 Select Enable CGI Execution under Site Options.
- 6 Click Save, then restart Web service.

Note: Note that for security reasons, the `printenv` and `test-cgi` scripts that are pre-installed in the /Library/WebServer/CGI-Executables folder are not executable by default. You may want to make them executable to verify correct operation of CGIs. Use either the Finder or the Terminal application to set their permissions to be executable.

Apple also supports CGIs written in AppleScript, referred to as ACGIs. To run an ACGI, use the Mac OS X Script Editor to save the AppleScript as an Application with the Stay Open option. Then start Classic and the ACGI Enabler (in /Applications/Utilities) before you request the file from a browser.

Enabling Server Side Includes (SSI)

Enabling Server Side Includes (SSI) allows a chunk of HTML code or other information to be shared by different Web pages on your site. SSIs can also function like CGIs and execute commands or scripts on the server.

Note: Enabling SSI requires making changes to UNIX configuration files in the Terminal application. To enable SSI, you must be comfortable with typing UNIX commands and using a UNIX text editor.

To enable SSI:

- 1 In the Terminal application, use a text editor to edit `/etc/httpd/httpd_macosxserver.conf`
- 2 Add the following line to each virtual host for which you want SSI enabled:

```
Options Includes
```

To enable SSI for all virtual hosts, add the line outside any virtual host block.

- 3 In Server Settings, click Web and add “index.shtml” to the set of default index files for each virtual host.

By default, the `mime__macosxserver.conf` file maintained by server settings contains the following two lines:

```
AddHandler server-parsed shtml
AddType text/html shtml
```

If your SSI files use a file extension other than `.shtml` you should add that type to the `mime__macosxserver.conf` file. You can add MIME types in Server Settings from the MIME Types tab.

The changes take effect when you restart the Web service.

Monitoring Web Sites

You can use the Sites pane to check the status of your Web sites. The Sites pane shows

- whether a site is enabled
- the site’s DNS name and IP address
- the port being used for the site

Double-clicking a site in the Sites pane opens the site settings window, where you can view or change the settings for the site.

To access the Sites pane:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.

Setting Server Responses to MIME Types

Multipurpose Internet Mail Extension (MIME) is 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 data in the file. Each suffix and its associated response together are called a “MIME type mapping.” See “Understanding Multipurpose Internet Mail Extension (MIME)” on page 340 for more information.

To set the server response for a MIME type:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the MIME Types tab and then click Add, or select a MIME type and click Edit.
- 4 Type the file suffix associated with this mapping in the File Suffix field.

- 5 Choose the server response from the pop-up menu, or type the file type in the Return MIME Type field.
If you return a CGI, make sure you've enabled CGI execution for the Web site.
- 6 Click Save, then restart Web service.

Enabling SSL

Before you can enable Secure Sockets Layer (SSL) protection for a Web site, you have to obtain the proper certificates.

For more information see “Setting Up Secure Sockets Layer (SSL) Service” on page 361.

To set up SSL for a Web site:

- 1 In Server Settings, click the Internet tab.
- 2 Click Web and choose Configure Web Service.
- 3 Click the Sites tab.
- 4 Select a site and click Edit.
- 5 Click the Security tab, then select Enable Secure Sockets Layer (SSL).
- 6 Click each button in the Security pane and paste the contents of the appropriate certificate or key in the text field for each. Click Save before going on to the next button.
- 7 Type the location of the SSL log file in the SSL Log File field.

You can also click the Select button and browse for the folder you want to use.

If you are administering a remote server, file service must be running on the local machine to use the Select button.

- 8 Click Save, then restart Web service.

Enabling PHP

PHP (PHP: Hypertext Preprocessor) is a scripting language embedded in HTML that is used to create dynamic Web pages. PHP provides functions similar to those of CGI scripts, but supports a variety of database formats and can communicate across networks via many different protocols. The PHP libraries are included in Mac OS X Server, but are disabled by default.

See “Installing and Viewing Web Modules” on page 365 for more information on PHP.

Note: Enabling PHP requires making changes to UNIX configuration files in the Terminal application. To enable PHP, you must be comfortable with typing UNIX commands and using a UNIX text editor.

To enable PHP:

- 1 In the Terminal application, use a text editor to edit `/etc/httpd/httpd.conf`
- 2 Enable PHP by removing the comment character, `#`, from the following lines, which are located in various places in the file:

```
#LoadModule php4_module /usr/libexec/httpd/libphp4.so  
#AddModule mod_php4.c
```

- 3 Save the changes and close the file.

The changes take effect when you restart the Web service.

WebMail

WebMail adds basic email functions to your Web site. If your Web service hosts more than one Web site, WebMail can provide access to mail service on any or all of the sites. The mail service looks the same on all sites.

The WebMail software is included in Mac OS X Server, but is disabled by default.

Note: Enabling WebMail requires making changes to UNIX configuration files in the Terminal application. To enable WebMail, you must be comfortable with typing UNIX commands and using a UNIX text editor.

The WebMail software is based on SquirrelMail, which is a collection of open-source scripts run by the Apache server. For more information on SquirrelMail, see this Web site:

www.squirrelmail.org

WebMail Users

If you enable WebMail, a Web browser user can

- compose messages and send them
- receive messages
- forward or reply to received messages
- maintain a signature that is automatically appended to each sent message
- create, delete, and rename folders and move messages between folders
- attach files to outgoing messages
- retrieve attached files from incoming messages
- manage a private address book
- set WebMail preferences, including the color scheme displayed in the Web browser

To use your WebMail service, a user must have an account on your mail server. Therefore, you must have a mail server set up if you want to offer WebMail on your Web sites.

Users access your Web site's WebMail page by appending /WebMail to the URL of your site. For example,

<http://mysite.example.com/WebMail>

Users log into WebMail with the name and password they use for logging in to regular mail service. WebMail does not provide its own authentication. For more information on mail service users, see “Supporting Mail Users” on page 405 in Chapter 9, “Mail Service.”

When users log in to WebMail, their passwords are sent over the Internet in clear text (not encrypted) unless the Web site is configured to use SSL. For instructions on configuring SSL, see “Enabling SSL for Web Service” on page 346.

WebMail users can consult the user manual for SquirrelMail at the following Web page:

www.squirrelmail.org/wiki/UserManual

WebMail and Your Mail Server

WebMail relies on your mail server to provide the actual mail service. WebMail merely provides access to the mail service through a Web browser. WebMail cannot provide mail service independent of a mail server.

WebMail uses the mail service of your Mac OS X Server by default. You can designate a different mail server if you are comfortable using the Terminal application and UNIX command-line tools. For instructions, see “Configuring WebMail” on page 360.

WebMail Protocols

WebMail uses standard email protocols and requires your mail server to support them:

- Internet Message Access Protocol (IMAP) for retrieving incoming mail
- Simple Mail Transfer Protocol (SMTP) for exchanging mail with other mail servers (sending outgoing mail and receiving incoming mail)

WebMail does not support retrieving incoming mail via Post Office Protocol (POP). Even if your mail server supports POP, WebMail does not.

Enabling WebMail

You can enable WebMail for the Web site (or sites) hosted by your Web service. Changes take effect when you restart Web service.

- 1** Make sure your mail service is started and configured to provide IMAP and SMTP service.
The mail service of Mac OS X Server provides IMAP and SMTP service by default. For details on mail service configuration, see Chapter 9, “Mail Service.”
- 2** Make sure IMAP mail service is enabled in the user accounts of the users you want to have WebMail access.

For details on mail settings in user accounts, see “Working With Mail Settings for Users” on page 150 in Chapter 3, “Users and Groups.”

- 3 Enable PHP according to the instructions on page 357.
- 4 In the Terminal application, use a text editor to edit `/etc/httpd/httpd_macosxserver.conf` and add the following line:

```
Include /etc/httpd/httpd_squirrelmail.conf
```

Where you add this line depends on whether your server hosts multiple Web sites and whether you want all or some hosted Web sites to have WebMail.

If your server hosts only one Web site or you want all Web sites to have WebMail, add the “Include” line outside all `<Virtual Host>` blocks.

If you want only some Web sites hosted by your server to have WebMail, add the “Include” line at or near the top of the `<Virtual Host>` block for each of your Web sites that you want to have WebMail service.

Here is an example of the beginning of a `<Virtual Host>` block for a Web site at 192.0.32.72 with the “Include” line added:

```
<VirtualHost 192.0.32.72:16080>
ServerName www.example.com
Include /etc/httpd/httpd_squirrelmail.conf
```

- 5 Add the default document name “index.php” to the default documents for the site.

This allows the server to display the default WebMail page if a client requests a URL for a folder without including a document name. See “Setting the Default Page for a Web Site” on page 351 for more information on adding a default document name.

Configuring WebMail

WebMail is based on SquirrelMail, an open-source module for the Apache Web server that provides Web service for Mac OS X Server. SquirrelMail has several options that you can configure to integrate WebMail with your site. The options and their default settings are as follows:

- Organization Name is displayed on the main WebMail page when a user logs in. The default is Mac OS X Server WebMail.
- Organization Logo specifies the relative or absolute path to an image file.
- Organization Title is displayed as the title of the Web browser window while viewing a WebMail page. The default is Mac OS X Server WebMail.
- Trash Folder is the name of the IMAP folder where mail service puts messages when the user deletes them. The default is Deleted Messages.

- Sent Folder is the name of the IMAP folder where mail service puts messages after sending them. The default is Sent Messages.
- Draft Folder is the name of the IMAP folder where mail service puts the user's draft messages. The default is Drafts.

You can configure these and other settings—such as which mail server provides mail service for WebMail—by running an interactive Perl script in a Terminal window, with root privileges. These configuration settings apply to all Web sites hosted by your Web service.

To configure basic WebMail options:

- 1 In the Terminal application, type

```
cd /opt/squirrelmail/configure  
sudo ./conf.pl
```

- 2 Follow the instructions displayed in the Terminal window.

WebMail configuration changes do not require restarting Web service unless users are logged in to WebMail.

To further customize the appearance (for example, to provide a specific appearance for each of your Web sites), you need to know how to write PHP scripts. In addition, you need to become familiar with the SquirrelMail plug-in architecture and write your own SquirrelMail plug-ins.

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. 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.

Generating 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 passphrase, then press Return.
The passphrase you create unlocks the server's certificate key. You will use this passphrase when you enable SSL on your Web server.
- 4 If it doesn't already exist on your server, create a directory at the following location:

```
/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 ssl.key directory.

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

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

This generates a file named csr.pem in your home directory.

- 6 When prompted, enter the following information:
 - *Country*: The country in which your organization is located.
 - *State*: The full name of your state.
 - *Locality*: The city in which your organization is located.
 - *Organizational name*: The organization to which your domain name is registered.
 - *Organizational unit*: Usually something similar to a department name.
 - *Common name of your Web server*: 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.

- 7 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).

Obtaining 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 SSLey.
- You have 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`.

Installing the Certificate on Your Server

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

Enabling SSL for the Site

- 1 In Server Settings, 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 Click the Security tab.
- 5 Select Enable Secure Socket Layer (SSL).
- 6 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.
- 7 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.
- 8 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.
- 9 Click in the Pass Phrase field and type the passphrase from your CSR in the text field, then click Save.
- 10 Set the location of the log file that will record SSL transactions and click Save.
- 11 Stop and then start Web service.

Solving Problems

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 at:
www.apache.org
- Check the Apache access and error logs.
- 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 the TCP/IP settings appear correct, 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.

A Web Module Is Not Working as Expected

- Check the error log in Server Status 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 is 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/

A CGI Will Not Run

- Check the CGI's file permissions to make sure the CGI is executable by www. If not, the CGI won't run on your server even if you enable CGI execution in Server Settings.

Installing and Viewing 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 this Web site:

www.apache.org/docs/mod

- To view a list of Web modules installed on your server, click Web in Server Settings, click Internet, click Web then select Show 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 the Finder, you can provide a search field for users to search your Web site.

- Choose Get Info in the Finder to index a folder’s contents.

Note: You must be logged in as root for the index to be copied to the Web directory in order to be searchable by a browser.

Clients must add `.sherlock` to your Web site’s URL to access a page that allows them to search your site. For example:

`http://www.example.com/.sherlock`

`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.

mod_redirectacgi_apple

This module works in conjunction with the ACgi Enabler Application to allow users to execute ACgi programs (Mac OS CGIs). To enable an ACgi, log in as the administrator and open the 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, and mod_perl.

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. See “Starting Tomcat” on page 347 for instructions.

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. PHP is also used to implement WebMail on Mac OS X Server. For more information about this module, see

www.php.net

mod_perl

This module integrates the complete Perl interpreter into the Web server, letting existing Perl CGI scripts run without modification. This integration means that the scripts run faster and consume fewer system resources. For more information about this module, see

perl.apache.org

MySQL

MySQL provides a relational database management solution for your Web server. With this open-source software, you can link data in different tables or databases and provide the information on your Web site.

The MySQL Manager application simplifies setting up the MySQL database on Mac OS X Server. You can use MySQL Manager to initialize the MySQL database, and to start and stop the MySQL service.

MySQL is pre-installed on Mac OS X Server, with its various files already in the appropriate locations. At some point you may wish to upgrade to a newer version of MySQL. You may install the new version in `/usr/local/mysql`, however, MySQL Manager will not be aware of the new version of MySQL and will continue to control the pre-installed version. If you do install a newer version of MySQL, use MySQL Manager to stop the pre-installed version, then start the newer version via the config file.

For more information on MySQL, see

www.mysql.com

Where to Find More Information

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

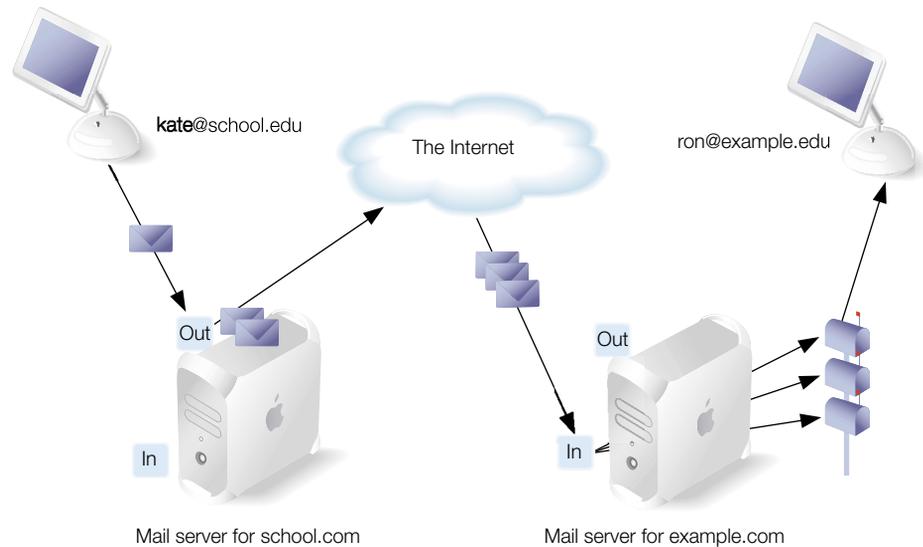
Mail service in Mac OS X Server allows network users to send and receive email over your network or across the Internet. The mail service sends and receives email using the standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP). The mail service also uses a Domain Name System (DNS) service to determine the address of outgoing mail.

This chapter begins with a look at the standard protocols used for sending and receiving email. It goes on to explain how mail service works, summarize the aspects of mail service management, and tell you how to

- manage mail service
- manage incoming and outgoing mail
- manage the mail database
- monitor and log mail activity
- limit junk mail
- handle undeliverable mail
- support mail users
- improve mail service performance
- back up and restore mail files

Mail Service Protocols

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



Post Office Protocol (POP)

The Post Office Protocol (POP) is used only for receiving mail, not for sending mail. The mail service of Mac OS X Server stores incoming POP mail until users have their computers connect to the mail service and download their waiting mail. After a user's computer downloads POP mail, the mail is stored only on the user's computer. The user's computer disconnects from the mail service, and the user can read, organize, and reply to the received POP mail. The POP service is like a post office, storing mail and delivering it to a specific address.

One advantage of POP is that your server doesn't need to store mail that users have downloaded. Therefore, your server doesn't need as much storage space as it would using 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 more than one computer, such as a home computer, an office computer, or a laptop while on the road. When a user reads mail via the POP protocol, the mail is downloaded to the user's computer 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 (IMAP)

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

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

Simple Mail Transfer Protocol (SMTP)

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

SMTP Alternatives: Sendmail and Postfix

Instead of the SMTP mail service of Mac OS X Server, you can use another *mail transfer agent (MTA)*, such as the UNIX programs Sendmail and Postfix. If you choose to use another mail transfer agent, it handles all incoming and outgoing SMTP mail. In this case, mail sent to local email users is delivered to the other mail transfer agent. Then Mac OS X Server transfers incoming mail from the other mail transfer agent for final delivery to email users using the POP and IMAP protocols. POP and IMAP continue to function as usual, but SMTP mail is now subject to the rules and settings of the other mail transfer agent.

The UNIX Sendmail program is included with Mac OS X Server and is configured to work correctly with Mac OS X Server mail service. To use Sendmail, you must set Mac OS X Server mail service to use an alternate mail transfer agent and you must start Sendmail. For more information about Sendmail, see this Web site:

www.sendmail.org

If you want to use the Postfix program instead of Sendmail, you must install and configure Postfix. Then you must set Mac OS X Server mail service to use an alternate mail transfer agent and you must start Postfix. For more information about Postfix, see this Web site:

www.postfix.org

How Mail Service Uses SSL

The mail service supports secure IMAP connections with mail client software that requests them. If a mail client requests a Secure Sockets Layer (SSL) connection, the mail service automatically complies. The mail service still provides non-SSL (unencrypted) connections to clients that do not request SSL. The mail service does not require any configuration to use SSL in this manner. The configuration of each mail client determines whether it connects with SSL or not.

How Mail Service Uses DNS

Before sending an email, your mail service will probably have a Domain Name System (DNS) service determine the Internet Protocol (IP) address of the destination. The DNS service is necessary because people typically address their outgoing mail by using a domain name, such as example.com, rather than an IP address, such as 198.162.12.12. To send an outgoing message, your mail service must know the IP address of the destination. The mail service relies on a DNS service to look up domain names and determine the corresponding IP addresses. The DNS service may be provided by your Internet service provider (ISP) or by Mac OS X Server, as explained in Chapter 14, “DNS Service.”

The mail that your mail service receives comes from other servers, and they use DNS to look up your mail service. DNS is able to find your mail service if you have created a mail exchange (MX) record for it. Your MX record specifies the name of the computer that handles mail service for your domain. This computer is known as a *mail host*. For example, the MX record for the domain example.com may specify that the name of the mail host is mail.example.com. If a mail service wants to send mail that’s addressed to someone@example.com, the mail service requests the MX record for the domain example.com and learns that it should actually send the mail to someone@mail.example.com.

An MX record can provide redundancy by listing an alternate mail host for a domain. If the primary mail host is not available, the mail can be sent to the alternate mail host. In fact, an MX record can list several mail hosts, each with a priority number. If the lowest priority host is busy, mail can be sent to the host with the next lowest priority, and so on.

Where Mail Is Stored

The mail service keeps track of email messages in a small database, but the database does not contain the messages. The mail service stores each message as a separate file in a mail folder. The mail service stores its database file and folder of messages in the folder `/Library/AppleMailServer` by default. You can change the location of the mail folder and database to another folder, disk, or disk partition. You can even specify a shared volume on another server as the location of the mail folder and database, although using a shared volume incurs performance penalties.

Mail service uses an additional folder if you turn on the option to use an alternate mail transfer agent, such as the UNIX Sendmail program. The alternate mail transfer agent delivers mail for users of your Apple mail service to the `/var/mail` folder. This is the standard UNIX mail delivery location. Mail for each user is stored in standard UNIX mailbox format in a file with the user's name. The Apple IMAP and POP service imports mail from this location to the mail database in the `/Library/AppleMailServer` folder. A user's mail remains in `/var/mail` until the user checks for new mail. Technically, the Apple mail service imports a user's mail when the user selects the Inbox via IMAP or triggers a LIST via POP.

How User Account Settings Affect Mail Service

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

- enable or disable mail service for the user account
- specify the server that provides mail service for the user account
- set a quota on the amount of disk space for storing the user account's mail on the server
- specify the protocol for the user account's incoming mail: POP, IMAP, or both
- maintain separate inboxes for POP and IMAP mail
- show a POP mailbox in the user's list of IMAP folders
- alert the user via NotifyMail when mail arrives

What Mail Service Can Do About Junk Mail

You can configure your mail service to decrease the volume of unsolicited mail, also known as junk mail and *spam*. You can take steps to block spam that is sent to your mail users.

You can also take steps to prevent senders of junk mail from using your server as a relay point. A *relay point* or *open relay* is a server that unselectively receives and forwards all mail addressed to other servers. An open relay sends mail from any domain to any domain. Junk mail senders exploit open relay servers to avoid having their own SMTP servers blacklisted as sources of spam. You do not want your server blacklisted as an open relay, because other servers may reject mail from your users.

Your mail service can do any of the following to reduce spam:

- require SMTP authentication
- restrict SMTP relay, allowing relay only by approved servers
- reject all SMTP connections from disapproved servers
- match the DNS name of every mail server to the reverse-lookup of its IP address
- reject mail from blacklisted servers

SMTP Authentication

If your mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server. SMTP authentication applies to mail relay, but does not apply to delivery of mail for local mail service users. Your mail service always accepts mail for local delivery without SMTP authentication.

Your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they will be unable to send mail.

Restricted SMTP Relay

If your mail service allows SMTP relay only by approved mail servers, then the approved servers can relay through your mail service without authenticating. You create the list of approved servers. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All mail servers, approved or not, can deliver mail to your local mail users without authenticating.

SMTP Authentication and Restricted SMTP Relay Combinations

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

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

Rejected SMTP Servers

You can have your mail service reject all SMTP connections from mail servers that you add to a list of disapproved servers. Your mail service does not allow anyone to authenticate from a disapproved server. No one can send your users mail or relay mail through your server from a disapproved server.

Mismatched DNS Name and IP Address

Your mail service can log and optionally reject connections from a mail server whose DNS name doesn't match the name that your DNS service gets when it looks up the mail server's IP address. This method intercepts junk mail from senders who pretend to be someone else, but may also block mail sent from a misconfigured SMTP server.

You should be aware that because reverse-lookups of IP addresses involve contacting DNS, they could slow down the performance of your mail service.

Blacklisted Servers

Your mail service can reject mail from SMTP servers that are blacklisted as open relays by an Open Relay Behavior-modification System (ORBS) server. Your mail service uses an ORBS server that you specify. ORBS servers are also known as *black-hole servers*.

What Mail Service Doesn't Do

Mail service provided by Mac OS X Server does not support

- mailing lists
- virtual domains (user@example1.com and user@example2.com can't be different mail accounts)
- Secure Sockets Layer (SSL) for SMTP and POP
- mail services on multiple Mac OS X Servers, because they would all try to provide SMTP service on port 25 and user accounts can't be assigned to a particular server for SMTP service

Mail Service Configuration in the Local Directory

The mail service configuration is stored in the local Open Directory domain of your Mac OS X Server, in a specific record with specific attributes and values. For example, the server's local Open Directory domain stores the path of the UNIX mail delivery location that is used if you choose to use a mail transfer agent other than the SMTP service of Mac OS X Server.

You can view and change the values of mail service attributes in the server's local Open Directory domain with NetInfo Manager, which is included with Mac OS X Server. For instructions, see "Using NetInfo Domains" on page 110 of Chapter 2, "Directory Services."

Overview of Mail Service Tools

The following applications help you set up and manage mail service.

- *Server Assistant*. Use to start mail service when you install Mac OS X Server
- *Server Settings*. Use to start, stop, and configure mail service
- *Workgroup Manager*. Use to create user accounts for email users and configure each user's mail options
- *Server Status*. Use to monitor mail service, view mail logs, list email accounts, and list connected email users
- *Terminal*. Optionally use for tasks that involve UNIX command-line tools, such as cleaning up the mail database and starting Sendmail

Setup Overview

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

- SMTP, POP, and IMAP all active and using standard ports
- standard authentication methods used (not Kerberos), with POP and IMAP set for clear-text passwords (APOP and CRAM-MD5 turned off) and SMTP authentication turned off
- local mail delivery only (no mail sent to the Internet)
- mail relay turned off
- administrator access via IMAP turned on

If you want to change this basic configuration, or if you have not set up your mail service, these are the major tasks you perform to set up mail service:

- Step 1: Before you begin, do some planning.
- Step 2: Set up MX records.
- Step 3: Start mail service.
- Step 4: Configure incoming mail service.
- Step 5: Configure outgoing mail service.
- Step 6: Configure additional settings for mail service.
- Step 7: Set up accounts for mail users.
- Step 8: Create a postmaster account.
- Step 9: Set up each user's mail client software.

Following is a summary of these tasks. The description of each task tells you which pages have detailed instructions for performing the task.

Step 1: Before you begin, do some planning

See “Before You Begin” on page 379 for a list of items to think about before you start full-scale mail service.

Step 2: Set up MX records

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

- If you have an Internet service provider (ISP) that provides DNS service to your network, contact the ISP and have the ISP set up MX records for you. Your ISP will need to know your mail server's DNS name (such as mail.example.com) and your server's IP address.

- If you use Mac OS X Server to provide DNS service, create your own MX records as described in “Using DNS With Mail Service” on page 516 in Chapter 14, “DNS Service.”
- If you do not set up an MX record for your mail server, your server may still be able to exchange mail with some other mail servers. Some mail servers will find your mail server by looking in DNS for your server’s A record. (You probably have an A record if you have a Web server set up.)

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

Step 3: Start mail service

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

Once you’ve verified this information, you can start mail service. If you selected the Server Assistant option to have mail service started automatically, stop mail service now and then start it again for your changes to take effect. For detailed instructions, see “Starting and Stopping Mail Service” on page 380.

Step 4: Configure incoming mail service

Your mail service has many settings that determine how it handles incoming mail. See these sections for instructions:

- “Working With Settings for Incoming Mail” on page 382
- “Working With Settings for Incoming POP Mail” on page 384
- “Working With Settings for Incoming IMAP Mail” on page 385

Step 5: Configure outgoing mail service

Your mail service also has many settings that determine how it handles outgoing mail. For instructions, see these sections:

- “Working With Settings for Outgoing Mail” on page 387
- “Working With Settings for SMTP Mail” on page 389

Step 6: Configure additional settings for mail service

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

- “Working With the Mail Database” on page 393
- “Cleaning Up the Mail Files” on page 395

- “Limiting Junk Mail” on page 398
- “Working With Undeliverable Mail” on page 402

Step 7: Set up accounts for mail users

Each person who wants mail service must have a user account in a directory domain accessible by your mail service. The short name of the user account is the mail account name and is used to form the user’s mail address. In addition, each user account has settings that determine how your mail service handles mail for the user account. You can configure a user’s mail settings when you create the user’s account, and you can change an existing user’s mail settings at any time. For instructions, see

- “Administering User Accounts” on page 137 of Chapter 3
- “Working With Mail Settings for Users” on page 150 of Chapter 3

Step 8: Create a postmaster account

You need to create a user account named “postmaster.” The mail service may send reports to the postmaster account. When you create the postmaster account, make sure mail service is enabled for it. For convenience, you can set up forwarding of the postmaster’s mail to another mail account that you check regularly. Chapter 3, “Users and Groups,” tells you how to create user accounts.

Step 9: Set up each user’s mail client software

After you set up mail service on your server, mail users must configure their mail client software for your mail service. For details about the facts that users need when configuring their mail client software, see “Supporting Mail Users” on page 405.

Overview of Ongoing Mail Service Management

Information in these sections will help you with your day-to-day mail service maintenance activities:

- “Monitoring Mail Status” on page 403
- “Performance Tuning” on page 407
- “Backing Up and Restoring Mail Files” on page 408

Before You Begin

Before setting up mail service for the first time:

- Decide whether to use POP, IMAP, or both for incoming mail.

- If your server will provide mail service over the Internet, you need a registered domain name. You also need to determine whether your ISP will create your MX records or you will create them in your own DNS service.
- Identify the people who will use your mail service but don't already have user accounts in a directory domain accessible to your mail service. You will have to create user accounts for these mail users.

Working With General Settings for Mail Service

This section tells you how to start and stop mail service, configure Kerberos authentication, list your mail server's local names, change any mail protocol settings, and monitor or archive mail. These settings affect all incoming and outgoing mail service protocols—POP, IMAP, and SMTP. All these settings are described in this section.

Starting and Stopping Mail Service

Mail service is ordinarily started automatically after you complete the Server Assistant. You can also use the Server Settings application to start and stop mail service at your discretion.

To start or stop mail service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Start Mail Service or Stop Mail Service.

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

When you start mail service, it looks for an existing database from an earlier version of Mac OS X Server. Mail service automatically converts an existing mail database and renames the existing database so that it won't be converted again. See “Converting the Mail Database From an Earlier Version” on page 393 for additional information.

Starting Mail Service Automatically

You can set mail service to start automatically whenever the Mac OS X Server system starts up. This ensures that mail service will start when the system restarts after a power outage or another unexpected event.

To configure automatic startup for mail service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the General tab.
- 4 Select “Start mail server at system startup” and click Save.

Requiring or Allowing Kerberos Authentication

You can choose to require, allow, or disallow the Kerberos authentication method for all SMTP, IMAP, and POP mail service.

Before enabling Kerberos authentication for mail service, you must integrate Mac OS X with a Kerberos server. For instructions, see “Integrating Mac OS X With a Kerberos Server” on page 199 in Chapter 3, “Users and Groups.”

To enable Kerberos authentication of mail service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the General tab.
- 4 Choose a method from the Authentication pop-up menu and click Save.

Choose Standard if you want mail service to use the authentication methods that are set by clicking POP Options, IMAP Options, and SMTP Options in the Protocols tab.

Choose Kerberos if you want mail service to require Kerberos authentication for POP, IMAP, and SMTP. In this case, users’ mail client software must support Kerberos.

Choose Any Method if you want to allow but not require the use of Kerberos authentication. A mail client that does not support Kerberos can use the standard authentication method instead.

Adding or Removing Local Names for the Mail Server

Your mail service has a list of all the domain names for which it is responsible. 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 all domain names in this list.

To add or remove local names for the mail server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click Add and type the domain name of a virtual mail host for which you want your server to be responsible.

To remove an item from the list, select it and click Remove.

- 4 Click Save.

Note: If you’ve set up MX records, you don’t need to add anything to this list. Your mail service 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, only your mail service recognizes it. External mail sent to this domain name will be returned. You should place domain names without MX records in this list only as a time saver for local (internal) mail.

Changing Protocol Settings for Mail Service

You can change the settings for all protocols that your mail service uses. These may include SMTP, IMAP, POP, and NotifyMail.

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab, then click the Options button for the protocol you want to change.
- 4 Make the changes you want and click Save.

Monitoring and Archiving Mail

You can configure mail service to send blind carbon copies of all messages to a user or group that you specify. You might want to do this if you need to monitor or archive messages. Senders and receivers of mail do not know that copies of their mail are being archived.

You can set up the specified user or group to receive the blind carbon copies using POP, and then set up a client email application to log in periodically and clean out the account by retrieving all new messages. You may want to set up filters in the email client to highlight certain types of messages. Or you may want to archive all messages for legal reasons.

To monitor or archive all messages:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Hosts.
- 3 Click the Incoming Mail tab.
- 4 Select “Blind copy incoming and outgoing messages to” and type a user name or group name.
- 5 Click Save.

Working With Settings for Incoming Mail

You can change settings that affect mail coming to users of your mail service, including mail your users receive from one another. The mail service has settings for limiting incoming message size, deleting incoming messages automatically, and notifying users who have new mail.

Limiting Incoming Message Size

You can set a maximum size for incoming messages. The default is 10,240 kilobytes (10 megabytes).

To set a maximum incoming message size:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Messages tab.
- 4 Select Message Size and type the number of kilobytes you want to set as the limit.
- 5 Click Save.

Deleting Email Automatically

You can have your mail service delete incoming messages automatically after a specified period of time. You may want to set these options if disk space is an issue.

Warning Automatic mail deletion permanently removes mail from the server, including messages in IMAP folders.

To delete incoming mail automatically:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Messages tab.
- 4 Select Automatic Mail Deletion and enter the number of days in the fields for unread and read mail.

Disable either setting by leaving it blank (don't enter a number of days). Disable all automatic mail deletion by deselecting Automatic Mail Deletion.

Notifying Users Who Have New Mail

Rather than require each user to periodically check for new mail, the mail service can notify users when they have new mail. To do this, you set your mail service to use the NotifyMail protocol.

To set your mail service to use NotifyMail:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable NotifyMail.
- 4 Click Save.

NotifyMail must also be enabled in each user account. For instructions, see “Enabling Mail Service Account Options” on page 150 of Chapter 3, “Users and Groups.”

In addition, third-party software must be installed on users’ computers. For more information, see this Web site:

www.notifymail.com

Working With Settings for Incoming POP Mail

Post Office Protocol (POP) is used to receive, but not send, mail. Users connect to a POP service to retrieve all of their waiting mail. After the user has retrieved mail, it is usually removed from the server. (A setting in the user’s mail client software determines whether it asks the POP service to remove the user’s retrieved mail.)

The mail service has settings for requiring authenticated POP connections, changing the POP response name, and changing the POP port number. All these settings are described in this section.

Requiring Authenticated POP (APOP)

Your POP mail service can protect users’ passwords by requiring APOP connections. When a user connects with APOP, the user’s mail client software encrypts the user’s password before sending it to your POP service. Before configuring your mail service to require APOP, make sure all users’ mail client software is able to use APOP as well.

To require APOP authentication:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable POP3, if it is not already checked.
- 4 Click POP3 Options.
- 5 Select “Require APOP authentication” and click Save.

Changing the POP Response Name

You can change the DNS name that your POP mail service sends back to a user’s mail client software when the client initiates a POP connection.

To change the POP response name:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable POP3, if it is not already checked.

- 4 Click POP3 Options.
- 5 Enter the DNS name you want your mail service to use when responding to POP connections, then click Save.

Changing the POP Port Number

The standard port number for POP mail service is 110. You can specify a different port, but do so carefully. If you change your mail service's POP port number, you must also change the POP port used by all users' mail client software. Also, don't use a port that is used by another service.

To change the POP port number:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable POP3, if it is not already checked.
- 4 Change the port number for the POP3 protocol and click Save.

Working With Settings for Incoming IMAP Mail

Internet Message Access Protocol (IMAP) is a client-server mail protocol that allows users to access their mail from anywhere on the Internet. Each IMAP user's mail remains in mailboxes on the server, just as if it were on the user's computer. IMAP delivers mail to the user's inbox as does POP, but when the user retrieves mail, it is not removed from the server.

The mail service has settings for requiring secure IMAP authentication, changing the IMAP response name, using case-sensitive IMAP folder names, controlling IMAP connections per user, terminating idle IMAP connections, and changing the IMAP port number. All these settings are described in this section.

Requiring Secure IMAP Authentication

Your IMAP mail service can protect users' passwords by requiring that connections use the Challenge-Response Authentication Method MD-5 (CRAM-MD5). When a user connects with CRAM-MD5 authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Before configuring your mail service to require CRAM-MD5 authentication, make sure all users' mail client software is able to authenticate using the CRAM-MD5 method.

To require CRAM-MD5 authentication:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.

- 3 Click the Protocols tab and select Enable IMAP, if it is not already checked.
- 4 Click IMAP Options.
- 5 Select “Require CRAM-MD5 authentication” and click Save.

Changing the IMAP Response Name

You can change the DNS name that your IMAP mail service sends back to a user’s mail client software when the client initiates an IMAP connection.

To change the IMAP response name:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable IMAP, if it is not already checked.
- 4 Click IMAP Options.
- 5 Enter the DNS name you want your mail service to use when responding to IMAP connections, then click Save.

Using Case-Sensitive IMAP Folder Names

You can allow mail users to create IMAP folders with names that are spelled the same but are capitalized differently. For example, a user could have one folder named “Urgent” and a different folder named “URGENT.”

To allow case-sensitive IMAP folder names:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable IMAP, if it is not already checked.
- 4 Click IMAP Options.
- 5 Select “Use case-sensitive IMAP folder names” and click Save.

Controlling IMAP Connections Per User

You can adjust the load each mail user can put on your server by limiting the number of connections each user can have on a single IP address.

To limit IMAP connections per user:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab, then click IMAP Options.

- 4 Enter the number of connections you want to allow, then click Save.

The default setting is 32, and the maximum is 128. A value of zero gives users unlimited connections.

Terminating Idle IMAP Connections

You can specify how long you want to allow IMAP mail connections to remain idle before the connection is terminated. Terminating idle connections can improve mail service performance.

To set idle connection limits:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab, then click IMAP Options.
- 4 Enter the number of minutes you want to allow for each IMAP connection, then click Save.

The default is 30 minutes, and a zero indicates that there is no time limit. The accepted range is 1 through 999.

Changing the IMAP Port Number

The default port for incoming IMAP connections is 143. You can change this port number, but you'll need to change the port number for IMAP client computers as well. Make sure you don't change to a port number already in use by another service or operation.

To change the IMAP port number:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable IMAP, if it is not already checked.
- 4 Change the port number for the IMAP protocol and click Save.

If you change your mail service's IMAP port number, you must also change the IMAP port used by all users' mail client software.

Working With Settings for Outgoing Mail

You can change settings that affect mail going out of your mail service, including mail that your users send to one another. The mail service has settings for sending nonlocal mail, sending only local mail, and suspending outgoing mail service.

Sending Nonlocal Mail

If your mail service currently allows sending only local mail, you can change a setting to allow sending mail to addresses outside your local network, including to the Internet.

To allow sending mail outside your local network:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Outgoing Mail tab.
- 4 Choose “Allow outgoing mail” from the pop-up menu, then click Save.

Sending Only Local Mail

You can set your mail service to allow sending only messages that are addressed to recipients on your local network. This setting prevents users from sending mail to addresses on the Internet.

To allow only local outgoing mail delivery:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Outgoing Mail tab.
- 4 Choose “Limit to local users” from the pop-up menu, then click Save.

If you limit outgoing mail to local users, all the options in the Outgoing Mail pane are disabled because they are not relevant to local outgoing mail.

Suspending Outgoing Mail Service

You can prevent the mail service from sending new outgoing mail. You could do this to isolate a problem, or to prevent conflicts with other mail service running on your network.

To suspend outgoing mail service:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and choose Use None from the pop-up menu.
- 4 Click Save.

Working With Settings for SMTP Mail

The mail service includes a Simple Mail Transfer Protocol (SMTP) service for sending mail. Subject to restrictions that you control, the SMTP service also transfers mail to and from mail service on other servers. If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service. Other mail services deliver messages for your mail users to your SMTP service, which then transfers the messages to your POP service and IMAP service.

Your mail service has settings for requiring SMTP authentication, sending mail via another SMTP server, changing the SMTP response names, changing the incoming SMTP port number, changing the outgoing SMTP port number, and enabling an alternate mail transfer agent. You can also start Sendmail. All these tasks are described in this section.

Your mail service also has settings that restrict SMTP mail transfer and thereby limit junk mail. For more information on these settings, see “Limiting Junk Mail” on page 398.

Requiring SMTP Authentication

Your server can guard against being an open relay by requiring SMTP authentication. Requiring authentication ensures that only known users—people with user accounts on your server—can send mail from your mail service. You can configure the mail service to require secure authentication using the CRAM-MD5 method. You can also allow the less secure PLAIN and LOGIN authentication methods, which don't encrypt passwords, if some users have email client software that doesn't support the CRAM-MD5 method.

Note: Requiring SMTP authentication does not affect delivery of mail to users of your mail service. Your mail service doesn't require other servers to authenticate before delivering mail for local mail service users.

To require SMTP authentication:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and Apple Mail Service SMTP from the pop-up menu.
- 4 Click SMTP Options.
- 5 Select “Require authenticated SMTP using CRAM-MD5,” optionally select “Allow PLAIN and LOGIN authentication,” and then click Save.

Sending SMTP Mail via Another Server

Rather than delivering outgoing mail directly to its various destinations, your SMTP mail service can relay outgoing mail to another server. The other server then attempts to deliver your SMTP service's outgoing mail. Your SMTP service batches outgoing mail and sends it to the other server, which acts as a proxy for delivering the mail.

- You may need to use this setting to deliver outgoing mail through a firewall set up by your organization. In this case, your organization will designate a particular server for relaying mail through the firewall.
- You may find this setting useful if your server has slow or intermittent connections to the Internet, or if you are billed by the number of connections you initiate.

To relay SMTP mail through another server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Outgoing Mail tab.
- 4 Click “Relay all SMTP mail via” and enter the DNS name or IP address of the server that provides SMTP relay.
- 5 Click Save.

Note: This option is disabled if the pop-up menu is set to “Limit to local users.”

Changing the SMTP Response Names

When your server connects with another server to send outgoing mail, your SMTP mail service identifies itself by sending a name. Your SMTP service also sends its name when another server contacts your server to deliver incoming mail. You can specify the name that your SMTP service sends for incoming connections and the name it sends for outgoing connections.

- The incoming and outgoing SMTP response names are typically the same.
- The incoming and outgoing response names should match the DNS name that another server would get by doing a reverse DNS lookup of your server’s IP address.
- If your server connects to the Internet via an Internet gateway or router that uses Network Address Translation (NAT), your server effectively has the IP address of the Internet gateway or router. In this case, the incoming and outgoing response names should match the DNS name that another server would get by doing a reverse DNS lookup of the Internet gateway’s IP address. An AirPort Base Station is an example of an Internet gateway that can be configured to use NAT.

To specify the SMTP response names:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and choose Apple Mail Service SMTP from the pop-up menu.
- 4 Click SMTP Options.
- 5 Enter the incoming response name and the outgoing response name, then click Save.

Changing the Incoming SMTP Port Number

You can change the port number on which your SMTP service receives incoming mail from other servers. Other servers must use this port number to deliver incoming mail to your server. The standard incoming SMTP port is 25. You can change this port number, but do so carefully. If you change to a nonstandard incoming SMTP port number, other servers will be unable to deliver incoming mail to your server unless they use this nonstandard port number for their outgoing SMTP mail. Make sure you don't change to a port number already in use by other services or operations.

To change the incoming SMTP port number:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable SMTP, if it is not already checked.
- 4 Change the port number for the SMTP protocol and click Save.

Changing the Outgoing SMTP Port Number

You can change the port number that your SMTP service uses when attempting to send outgoing mail to other servers. The standard port for outgoing SMTP connections is 25. You can change this port number, but do so carefully. If you use a nonstandard outgoing SMTP port, your server will be unable to deliver outgoing mail to other servers unless they use this nonstandard port for their incoming SMTP mail. Make sure you don't change to a port number already in use by another service or operation.

To change the outgoing SMTP port number:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Network Settings tab.
- 4 Change the SMTP port number and click Save.

Enabling an Alternate Mail Transfer Agent

You can use an alternate mail transfer agent, such as the UNIX Sendmail program, to handle incoming and outgoing SMTP mail. Any mail sent to local email users is processed by the mail transfer agent and transferred to the Mac OS X Server mail service for delivery. POP and IMAP continue to function as usual, but SMTP mail is now subject to the rules and settings of the mail transfer agent.

To use another mail transfer agent:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.

- 3 Click the Protocols tab and choose Other Mail Transfer Agent from the pop-up menu.
- 4 Click Save.
- 5 Start the other mail transfer agent program.

Starting Sendmail

If you configure mail service to use an alternate mail transfer agent such as the UNIX program Sendmail, you need to start the mail transfer agent program. It then becomes the primary SMTP mail transfer agent on your server.

The UNIX Sendmail program is included with Mac OS X. To start Sendmail as root, type this command in the Terminal application:

```
/usr/lib/sendmail -bd
```

To configure Sendmail to start automatically every time the system starts up, you need root privileges; edit the `/etc/hostconfig` file, find the line containing MAILSERVER, and make it read

```
MAILSERVER=-YES-
```

To keep Sendmail from starting when the system starts up, change the line to

```
MAILSERVER=-NO-
```

The Sendmail program will not operate if the permissions of the root directory are changed. Some installer programs for software updates or applications may change the root directory permissions from the standard for Mac OS X Server to the standard for a Mac OS X client computer.

The standard for Mac OS X Server is 1755 or `rwrx-xr-t`, which means read/write/execute by owner, read/execute by group, and read/execute by everyone (world).

The standard for a Mac OS X client is 1775 or `rwrxwxr-t`, which allows group write privileges.

You can check the permissions currently set for the root directory by typing the following command in the Terminal application:

```
ls -al /
```

This form of the `ls` command displays detailed information for the root directory. The first character of each line indicates the type of item (`d` for directory, `l` for symbolic link, `-` for regular file). This is followed by nine characters that indicate the permissions for the item. The item name is at the end of the line. A single period (`.`) represents the directory whose contents are listed, and it is the first line displayed by this `ls` command. In this case, the first line is for the root directory.

If the permissions for the root directory are `rwrr-xr-t` then they are correct for Mac OS X Server.

If the permissions for the root directory are `rw-rw-r-t` then they have been changed to the standard for a Mac OS X client. To correct this, type the following command in the Terminal application:

```
sudo chmod g-w /
```

For more information on Sendmail, see this Web site:

www.sendmail.org

Working With the Mail Database

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

- convert the mail database from an earlier version of Mac OS X Server
- change the location where the mail database and files are stored
- configure automatic mail deletion
- allow administrators to access the mail database and files via IMAP
- clean up the mail database and files

All these tasks are described in this section.

Converting the Mail Database From an Earlier Version

When mail service starts for the first time, it looks for an existing mail database from an earlier version of Mac OS X Server. Mail service migrates messages from an existing mail database to the current mail database format. After migrating all messages, mail service renames the old database to preclude the old database from being converted again. You can delete the renamed database file when you are satisfied that the migration and conversion process was successful.

In Mac OS X Server version 10.2, the mail service stores each message in a separate file and keeps track of message files in a relatively small database file. In earlier versions of Mac OS X Server, the mail service stores all messages in one large database file, `/Library/AppleMailServer/MacOSXMailDB`. The automatic conversion process extracts each message from the monolithic database file and stores it in a separate file. The message files are located in a folder at `/Library/AppleMailServer/AppleMail` (unless you change the location where mail is stored). The new `MacOSXMailDB` file contains only user and mail account information.

Note: For the mail database conversion to complete successfully, the server must have enough disk space available. The amount of disk space available should equal the size of the database file being converted.

Changing Where Mail Is Stored

You can change where mail is stored on the server. The default location is `/Library/AppleMailServer`.

To change where mail is stored on the server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the General tab.
- 4 Select “Use alternate mail store location” and enter the path of the location that you want to use.
- 5 Click Save.

Configuring Automatic Mail Deletion

If disk space is an issue, you can have read and unread mail automatically deleted from your server at specified times. If you choose this option, you should let your users know how long their messages will remain on the server before being deleted. Automatic mail deletion permanently removes mail from the server, including messages in IMAP folders.

To set up automatic mail deletion:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Messages tab.
- 4 Click Automatic Mail Deletion and type the number of days in the field below for unread mail and read mail.
Don't enter a number if you don't want to enable one of the settings.
- 5 Click Save.

Allowing Administrator Access to the Mail Database and Files

You can configure IMAP to allow the server administrator to view and modify any message in the mail database. To take advantage of this administrator access, you must use an email client that allows you to change its IMAP port number, such as the Mail application in Mac OS X. To gain administrator access from such an email client, you must know a server administrator name and password.

The mail client must be configured to use the IMAP administrator port instead of the normal IMAP port. The standard port number for IMAP administrator access is 626. You can change your mail service to use a different port number.

When your mail client connects on the IMAP administrator port, you see all the messages stored on the server. Each user's mailbox appears as a separate folder in your mail client. You can remove disused mailbox folders that belonged to deleted user accounts.

In addition to seeing the mail users, you also see outgoing mail hosts. A host with an unusually high number of messages queued for delivery may indicate that your mail service is unable to connect with the host to exchange mail.

If you allow administrator access to the mail database, you should use your server's IP firewall service to restrict connections on the IMAP administrator port (port 626 by default) to IP addresses that are well known to you. For instructions, see Chapter 15, "Firewall Service."

To configure administrator access to the database:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and select Enable IMAP, if it is not already checked.
- 4 Click IMAP Options.
- 5 Select Allow IMAP Administrator Access and optionally change the port number.
- 6 Click Save.
- 7 In your email client application, create an account that uses IMAP to connect to your mail service and change the IMAP port to match the port specified in step 5.

For example, to change an IMAP account's port number in the Mac OS X Mail application, choose Preferences from the Mail menu, click Accounts, select the IMAP account, click Edit, and click the Advanced tab. (If your version of Mail doesn't have an Advanced tab, click the Account Options tab.)

Cleaning Up the Mail Files

You can clean up and compact the mail database and other mail files by typing a simple UNIX command in the Terminal application.

Note: Cleaning up and compacting the mail files may take a long time. The length of time depends on the number of mail messages and the number of mail users.

To clean up and compact the mail database:

- 1 In Server Settings, stop mail service.
- 2 Open Terminal and at the prompt, type the following and then press Return:

```
sudo /usr/sbin/MailService -compressDB
```
- 3 Enter your administrator password and press Return.

The cleanup operation takes place without any feedback. During cleanup, a number of messages are written in the mail service repair log, which you can view by using Server Status. The cleanup operation is finished when another command-line prompt appears.

- 4 In Server Settings, start mail service.

Working With Network Settings for Mail Service

You can change the following network settings of your mail service:

- which DNS records mail service uses to look up a mail server
- when mail service updates its DNS cache
- when mail service connections time out

This section describes how to change these settings.

Specifying DNS Lookup for Mail Service

You can specify the type of DNS records you want your mail service to use when it looks up the server for an address of an outgoing message, such as `user@example.com`. Your mail service can look up another server by requesting

- *Only an MX list.* An MX List consists of one or more MX records for an Internet domain. An MX record matches a domain name, such as `example.com`, with the full DNS name of a mail server, such as `mail.example.com`. Some domains have more than one mail server, each with an MX record. In this case, the MX records specify priorities for the mail servers. Some mail servers don't have any MX records.
- *Only an A record.* An A record matches a full DNS name (also known as a host name), such as `mail.example.com`, to an IP address.
- *An MX list and an A record.* By default, your mail service requests MX records. If none exists, the mail service requests an A record.

To specify the type of DNS records your mail service requests:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Network Settings tab.
- 4 Select one of the settings for DNS Request, then click Save.

Updating the DNS Cache in Mail Service

The mail service stores verified domain names in a cache and does not verify the cached information unless you set the cache to be updated periodically. The cache improves mail service performance, because the mail service doesn't have to contact the DNS service for every message. You may reduce mail service performance if you set the cache to be updated too frequently.

To change how often the mail service updates its DNS cache:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Network Settings tab.
- 4 Select one of the Cache Settings options.

Select "Cache DNS information for ___ minutes" and enter the number of minutes you want information to be stored before the cache is refreshed.

Select "Respect 'Time to Live' (TTL) DNS Settings" if you want to use the default settings of the DNS service. Ordinarily, your mail service resends mail repeatedly until it makes a connection with the server at the destination. TTL specifies how long your mail service continues requesting connection information from DNS before giving up and generating a nondelivery report.

- 5 Click Save.

Changing Mail Service Timeouts

If your mail service has frequent trouble remaining connected to another server, you can increase the length of time your mail service waits before giving up on connections with other servers. This can be helpful if your server has a slow or intermittent connection to the Internet.

To change the allowed connection time:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Network Settings tab.
- 4 In the Open Connection field, enter the number of seconds you want your mail service to wait before giving up on a connection attempt.
- 5 In the Read/Write field, enter the number of seconds you want to allow the other mail host to respond before your mail service stops attempting to send or receive a message.
- 6 Click Save.

Limiting Junk Mail

You can configure mail settings to decrease the amount of junk mail that your mail service delivers to users. You can also take steps to prevent senders of junk mail (spam) from using your server as an open relay. If you allow junk mail senders to use your server as a relay point, your server may be blacklisted as an open relay, and other servers may reject mail from your users. Your mail service can do the following to reduce spam:

- Require SMTP authentication so that your server cannot be used as a relay point by anonymous users. For instructions, see “Requiring SMTP Authentication” on page 389.
- Restrict SMTP relay, allowing relay only by approved servers on a list that you create. For instructions, see “Restricting SMTP Relay” on page 398.
- Reject SMTP connections from specific servers on another list that you create. For instructions, see “Rejecting SMTP Connections From Specific Servers” on page 399.
- Log and optionally reject an SMTP connection from a server whose DNS name doesn’t match a reverse-lookup of its IP address. For instructions, see “Checking for Mismatched SMTP Server Name and IP Address” on page 399.
- Reject SMTP connections from servers that are blacklisted as open relays by an Open Relay Behavior-modification System (ORBS) server. For instructions, see “Rejecting Mail From Blacklisted Senders” on page 401.
- Allow or deny SMTP connections from specific IP addresses by using the firewall service of Mac OS X Server. For instructions, see “Filtering SMTP Connections” on page 401.

Restricting SMTP Relay

Your mail service can restrict SMTP relay by allowing only approved servers to relay mail. You create the list of approved servers. Approved servers can relay through your mail service without authenticating. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All servers, approved or not, can deliver mail to your local mail users without authenticating.

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

To restrict SMTP relay:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.
- 3 Click the Incoming Mail tab.
- 4 Select “only hosts in this list” and then edit the list of servers.

Click Add to add a server to the list.

Click Remove to delete the currently selected server from the list.

When adding to the list, you can use a variety of notations.

Enter a single IP address, such as 192.168.123.55.

Enter an IP address range, such as 192.168.40-43.*.

Enter an IP address/netmask, such as 192.168.40.0/255.255.248.0.

Enter a host name, such as mail.example.com

Enter an Internet domain name, such as example.com

- 5 Optionally select “Log recipient rejections to error log.”
- 6 Click Save.

Rejecting SMTP Connections From Specific Servers

Your mail service can reject all SMTP connections from servers on a disapproved-servers list that you create. No one can authenticate from a disapproved server, much less send your users mail or relay mail through your mail service.

To reject SMTP connections from specific servers:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Filter tab.
- 4 Select “Reject messages from SMTP servers in list” and then edit the list of servers.

Click Add to add a server to the list.

Click Remove to delete the currently selected server from the list.

When adding to the list, you can use a variety of notations.

Enter a single IP address, such as 192.168.123.55.

Enter an IP address range, such as 192.168.40-43.*.

Enter an IP address/netmask, such as 192.168.40.0/255.255.248.0.

Enter a host name, such as mail.example.com

Enter an Internet domain name, such as example.com

- 5 Click Save.

Checking for Mismatched SMTP Server Name and IP Address

Your mail service can log and optionally reject connections from a server whose DNS name doesn't match the name that your DNS service gets when it looks up the server's IP address. This method intercepts junk mail from senders who pretend to be someone else, but may also block mail sent from a misconfigured SMTP server.

Note: Reverse-lookups of IP addresses may slow the performance of your mail service because lookups involve more contact with DNS service.

To check SMTP server names and IP addresses:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Filter tab.
- 4 Select “Log connection if SMTP name does not match IP address” and then optionally select “Reject if name does not match address.”
- 5 Click Save.

Your SMTP mail service may be unable to do a successful reverse lookup of a server that identifies itself in a nonstandard way. Specifically, the SMTP service can determine the server name in a HELO command that doesn’t deviate too much from standard form.

The SMTP service can determine the server name and do a reverse lookup from HELO commands like the following:

```
helo mail.example.com
helo I am mail.example.com
```

The SMTP service cannot do a reverse lookup from HELO commands like the following:

```
helo I’m mail.example.com
helo I am mail server mail.example.com
helo what a wonderful day it is
```

The following table explains the results for various configurations of the settings for logging and rejecting unsuccessful reverse lookups.

Log	Reject	Result
No	No	Accepts all HELO commands
Yes	No	Accepts all HELO commands and logs each server whose name doesn’t match or whose name can’t be determined from the HELO command
Yes	Yes	Logs and rejects each server whose name doesn’t match or whose name can’t be determined from the HELO command

Rejecting Mail From Blacklisted Senders

You can have your mail service check an Open Relay Behavior-modification System (ORBS) server to see if incoming mail came from a known junk-mail sender. ORBS servers are also known as black-hole servers.

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

To reject mail from known junk-mail senders:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Filter tab.
- 4 Select “Use a server for junk mail rejection” and then type the DNS name of an ORBS server.
- 5 Click Save.

Allowing SMTP Relay for a Backup Mail Server

If your network has more than one mail server, one can be designated as a backup server to deliver mail in case the primary server goes down. (Backup mail servers are designated by MX records.) A backup mail server may need to relay SMTP mail. You can set your server to ignore SMTP relay restrictions when accepting mail as a backup server for another mail server.

To allow SMTP relay for a backup mail server:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and choose Apple Mail Service SMTP from the pop-up menu.
- 4 Click SMTP Options.
- 5 Select “SMTP relay when host is a backup for destination” and click Save.

Filtering SMTP Connections

You can use the firewall service of Mac OS X Server to allow or deny access to your SMTP mail service from specific IP addresses.

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Click New and configure the settings to create a filter that allows or denies access to port number 25 from an IP address or range of IP addresses that you specify, then click Save.

If your SMTP service does not use port 25, which is standard for incoming SMTP mail, enter your incoming SMTP port number instead.

- 4 Add more new filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information on the firewall service, see Chapter 15, “Firewall Service.”

Working With Undeliverable Mail

Mail messages may be undeliverable for several reasons. You can configure your mail service to forward undeliverable incoming mail, limit attempts to deliver problematic outgoing mail, and report failed delivery attempts. Incoming mail may be undeliverable because it has a misspelled address or is addressed to a deleted user account. Outgoing mail may be undeliverable because it’s misaddressed or the destination mail server is not working.

Forwarding Undeliverable Incoming Mail

You can have mail service forward messages that arrive for unknown local users to another person or a group in your organization. Whoever receives forwarded mail that’s incorrectly addressed (with a typo in the address, for example) can forward it to the correct recipient. If forwarding of these undeliverable messages is disabled, they are returned to sender.

To set up forwarding of undeliverable incoming mail:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Messages tab.
- 4 Select “Forward mail addressed to unknown local users” and type a user name or group name.
- 5 Click Save.

Limiting Delivery Attempts in Mail Service

You can limit how often and for how long your mail service attempts to deliver mail sent by your users. If mail can’t be delivered within the time you specify, the mail service sends a nondelivery report to the message sender and deletes the message. You can have the mail service send an earlier nondelivery report. You can also have a nondelivery report sent to the postmaster account.

To limit delivery attempts:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Host Settings.

- 3 Click the Outgoing Mail tab.
- 4 Enter the number of hours you want the mail service to attempt to deliver a message before the message expires.
The default is 72 hours.
- 5 Enter the number of minutes you want the mail service to wait between delivery attempts.
The smallest number allowed is 1 minute; the default is 20 minutes.
- 6 Optionally click “Notify sender of non-delivery after ___ hours” and enter the number of hours.
- 7 Optionally click “Notify postmaster of non-delivery.”
- 8 Click Save.

Note: These options are disabled if the pop-up menu is set to “Limit to local users.”

Sending Nondelivery Reports to Postmaster

When a user on your network sends mail that can't be delivered, a nondelivery report is sent back to the user. If for some reason the report can't be delivered, you can set up mail service to send the report to the postmaster account. Be sure you've set up a user account named “postmaster.”

Nondelivery reports are not normally sent for mail designated as “bulk,” but you can also generate nondelivery reports for bulk mailings.

To report undelivered mail to the postmaster account:

- 1 In Server Settings, click the Internet tab.
- 2 Click Mail Service and choose Configure Mail Service.
- 3 Click the Protocols tab and choose SMTP from the pop-up menu.
- 4 Click SMTP Options.
- 5 Click one or both of the nondelivery options, then click Save.

Monitoring Mail Status

This section explains how to use the Server Status application to monitor the following:

- overall mail service activity
- connected mail users
- mail accounts
- mail service logs

This section also describes how Mac OS X Server reclaims disk space used by logs and how you can reclaim space manually.

Viewing Overall Mail Service Activity

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

To see an overview of mail service activity:

- 1 In Server Status, select Mail in the Devices & Services list.
- 2 Click the Overview tab.

Viewing Connected Mail Users

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

To view a list of mail users who are currently connected:

- 1 In Server Status, select Mail in the Devices & Services list.
- 2 Click the Connections tab.

Viewing Mail Accounts

You can use the Server Status application to see a list of users who have mail accounts. For each account, you see the user name, disk space quota, disk space used, and the percent of space that is available to the user.

To view a list of mail accounts:

- 1 In Server Status, select Mail in the Devices & Services list.
- 2 Click the Accounts tab.

Reviewing Mail Service Logs

The mail service maintains eight logs, and you can use Server Status to view them.

- *IMAP, POP, SMTP In, and SMTP Out logs.* These four logs contain the history of activity that is specific to each protocol.
- *Router log.* Routing errors and routing messages go into the router log.
- *Error log.* General mail service errors go into the Error log.
- *Server log.* General mail service information goes into the server log.
- *Repair log.* This log contains a history of cleanup, compression, and repairs made to the mail database.

To view a mail service log:

- 1 In Server Status, select Mail in the Devices & Services list.
- 2 Click the Logs tab.
- 3 Choose a log from the Show pop-up menu.

Reclaiming Disk Space Used by Mail Service Logs

Mac OS X Server automatically reclaims disk space used by mail service logs when they reach a certain size or age. If you are comfortable using the Terminal application and UNIX command-line tools, you can change the criteria that determine when disk space is reclaimed. You can also use a command-line tool to monitor disk space whenever you want, independently of the automatic disk-space recovery process. For additional information, see “Log Rolling Scripts” on page 555 and “diskspacemonitor” on page 556, both in Chapter 17, “Tools for Advanced Users.”

Supporting Mail Users

This section discusses mail settings in your server’s user accounts and mail service settings in email client software.

Configuring Mail Settings for User Accounts

To make mail service available to users, you must configure mail settings in your user accounts. For each user, you need to enable mail service, enter the DNS name or IP address of your mail server, and select the protocols for retrieving incoming mail (POP, IMAP, or both). You can also set a quota on disk space available for storing a user’s mail. If you configure a user account for both POP and IMAP, additional options let you specify whether the user has separate inboxes for POP and IMAP and whether the POP mailbox appears in the IMAP folder list. One more option specifies whether mail service alerts the user via NotifyMail when mail arrives.

You configure these settings in the Accounts module of Workgroup Manager. For instructions, see “Working With Mail Settings for Users” on page 150 in Chapter 3, “Users and Groups.”

Configuring Email Client Software

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

Email client software	Mac OS X Server	Example
User name	Full name of the user	Steve Macintosh
Account name Account ID	Short name of user account	steve
Password	Password of user account	
Host name Mail server Mail host	Mail server's full DNS name or IP address, as used when you log in to the server in Server Settings	mail.example.com 192.168.50.1
Email address	User's short name, followed by the @ symbol, followed by one of the following: <ul style="list-style-type: none">■ Server's Internet domain (if the mail server has an MX record in DNS)■ Mail server's full DNS name■ Server's IP address	steve@example.com steve@mail.example.com steve@192.168.50.1
SMTP host SMTP server	Same as host name	mail.example.com 192.168.50.1
POP host POP server	Same as host name	mail.example.com 192.168.50.1
IMAP host IMAP server	Same as host name	mail.example.com 192.168.50.1
SMTP user	Short name of user account	steve
SMTP password	Password of user account	

Creating Additional Email Addresses for a User

Mail service allows each individual user to have more than one email address. Every user has one email address that is formed from the short name of the user account. In addition, you can define more short names for any user account by using Workgroup Manager. Each additional short name is an alternate email address for the user. The additional short names are called *virtual users*. For more information on defining additional short names, see “Defining Short Names” on page 140 in Chapter 3, “Users and Groups.”

Someone whose user account has multiple short names nonetheless has only one mail account. A user receives mail for all of the user’s short names in one mailbox. The user cannot set up a different mailbox (or different incoming mail accounts) for each short name. If a user needs an additional mailbox, you must create another user account.

Note: Mail service does not support virtual domains. For example, mail service cannot deliver mail for `webmaster@example1.com` to the same mailbox as mail for `webmaster@example2.com` if `example1.com` and `example2.com` have different IP addresses.

Performance Tuning

Mail service needs to act very fast for a short period of time. Mail service sits idle until a user wants to read or send a message, and then it needs to transfer the message immediately. Therefore, mail service does not put a heavy continuous demand on the server; it puts intense but brief demands on the server. As long as other services do not place heavy continuous demands on a server (as a QuickTime streaming server would, for example), the server can typically handle several hundred connected users.

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

- Adjust how often mail service updates its DNS cache. For instructions, see “Updating the DNS Cache in Mail Service” on page 397.
- Adjust the load each mail user can put on your server by limiting the number of connections each user can have on a single IP address. For instructions, see “Controlling IMAP Connections Per User” on page 386.
- Specify how long you want to allow IMAP mail connections to remain idle before the connection is terminated. For instructions, see “Terminating Idle IMAP Connections” on page 387.
- Move the mail storage location to its own hard disk or hard disk partition. For instructions, see “Changing Where Mail Is Stored” on page 394.
- Run other services on a different server, especially services that place frequent heavy demands on the server. (Each server requires a separate Mac OS X Server license.)

Backing Up and Restoring Mail Files

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

- MacOSXMailDatabase, which is the mail service database file
- AppleMail, which is the folder that contains a file for each mail message and a file for each mail account

These items are stored in the folder `/Library/AppleMailServer` unless you specify a different location. For instructions on changing the mail folder location, see “Changing Where Mail Is Stored” on page 394.

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

An incremental backup of the mail service folder can be fast and efficient. If you use a third-party application to back up the mail service folder incrementally, the only files copied are the small database file and the message files that are new or changed since the last backup.

Although you can restore only part of the mail service folder—some message files in the AppleMail folder with or without the MacOSXMailDatabase file—restoring only part of the mail service folder can corrupt the mail database. The mail service automatically attempts to clean up a mail service folder that has been restored improperly. You can also clean up the mail service folder manually. For instructions, see “Cleaning Up the Mail Files” on page 395.

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

If you’re using the UNIX Sendmail program or another mail transfer agent instead of Mac OS X Server’s SMTP service, you should also back up the contents of the `/var/mail` folder. This folder is the standard location for UNIX mail delivery.

Where to Find More Information

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

Books

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

- A good 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).

Internet

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 will probably find some of the background information in an RFC helpful. If you are an experienced server administrator, you can find all the 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 more information about Sendmail, see this Web site:

www.sendmail.org

You can find out more about servers that filter junk mail at this Web site:

www.ordb.org

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.

Client Management: Mac OS 9 and OS 8

Macintosh Manager provides network administrators with a centralized method of managing Mac OS 9 and Mac OS 8 workstations, controlling access to software and removable media, and providing a consistent, personalized experience for users. After you import basic information (user name, password, and user ID) from Workgroup Manager user accounts, you can customize preferences and privileges for users, workgroups, and computer lists. Mac OS X Server saves user documents and preferences in a home directory, so your users can access their files from any Mac on your network.

Like Workgroup Manager, Macintosh Manager lets you set network-wide policies for controlling user access to applications, file server volumes, and printers. Macintosh Manager provides its own authentication and preference management for Mac OS 9 or Mac OS 8 computers and can be used with NetBoot clients.

Client management can help you create a more tailored and efficient user experience. Because you can define the user environment, you can provide an interface suitable for users with different skill levels. This can make it easier, for example, to set up an elementary school computer lab for use by a wide range of students from kindergarten to eighth grade.

This chapter summarizes how Macintosh Manager works, gives details about different types of managed environments, and tells you how to

- set up Macintosh Manager
- import users into Macintosh Manager
- set up workgroups and computer lists for Mac OS 9 and OS 8 clients
- create managed environments for Mac OS 9 and OS 8 clients
- implement Macintosh Manager security settings and controls

Note: Macintosh Manager is not used to manage Mac OS X clients. If you need to manage Mac OS X clients, read Chapter 6, “Client Management: Mac OS X.”

Transition Strategies for Macintosh Manager

If you are migrating to Macintosh Manager 2.2 from an earlier version, you can do a simple upgrade to the new Macintosh Manager. Functionality remains much the same, but you may notice some differences in how Macintosh Manager stores certain items.

If you need more information about migration issues and strategies, download the “Upgrading to Mac OS X Server” from the Web site listed below:

www.apple.com/macosx/server/

The User Experience

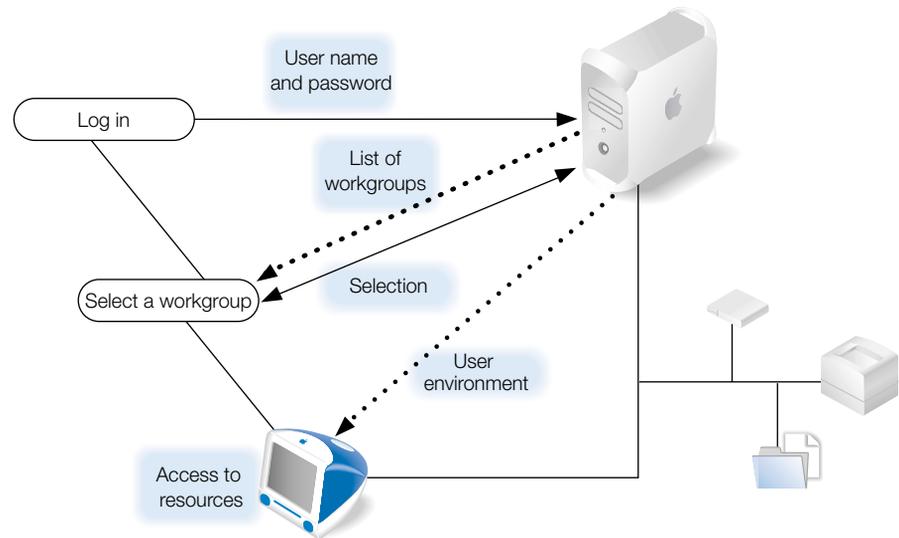
This section describes both the actual user experience and the server processes for Mac OS 9 managed clients.

Logging In

Users imported into Macintosh Manager can simply type their Mac OS X Server user names and passwords in the Macintosh Manager login dialog box. Alternatively, you can allow users to choose their names from a list (showing long names) at login.

When a user logs in, Macintosh Manager uses Directory Services to verify that the user ID is valid. If it is valid, Macintosh Manager finds the correct workgroups for that user and displays them in a list. If a user belongs to more than one workgroup, he or she can select a workgroup from the list. If a user belongs to only one workgroup, login proceeds automatically without displaying a workgroup list. Macintosh Manager workgroup settings define the user’s working environment (Finder, Restricted Finder, or Panels).

Depending upon the computer being used, the network configuration, and access privileges, the user may have access to various resources such as printers, applications, and volumes. Settings for the computer, the workgroup, and the user determine the final set of privileges and preferences that define the user experience for an individual.



Logging In Using the All Other Users Account

Users who have a Mac OS X user account but have not been imported into Macintosh Manager can type their Mac OS X Server user names and passwords in the Macintosh Manager login dialog box. If the All Other Users account belongs to more than one workgroup, the user can select a workgroup from a list. Otherwise, login continues automatically.

Logging In Using the Guest Account

Any user can log in as Guest, provided that the Guest account has been activated. The Guest account does not require password authentication. If the Guest account belongs to more than one workgroup, the user can select a workgroup from a list. Otherwise, login continues automatically.

Locating the Home Directory

User home directories are mounted automatically when a user logs in. A folder with the user's name on it appears on the desktop or on a panel depending upon the workgroup type. The user's home directory is located inside the Users folder.

Guest users have a temporary local home directory for storing files or preferences.

Finding Applications

Approved applications for Panels and Restricted Finder workgroups are located in the “Items for *workgroup name*” folder inside the user’s home directory. For users in a Finder workgroup, applications are stored in the client computer’s Applications folder or Applications (Mac OS 9) folder.

Finding Shared Documents

Depending on the user environment and how you set up workgroup folders, users may have access to several areas where they can view or store shared items. For example, you can set up a group documents volume inside the Macintosh Manager sharepoint to allow users to collaborate more effectively, or you might provide a hand-in folder for a Panels workgroup to allow users to turn in documents.

Before You Begin

You should consider taking advantage of client management if

- you want to provide users with a consistent, controlled interface while allowing them to access their documents from any computer
- you want to control privileges for users with mobile computers
- you want to reserve certain resources for only specific groups or individuals
- you need to secure computer usage in key areas such as administrative offices, classrooms, or open labs

Before you set up Macintosh Manager to manage users, groups, or computers, be sure to follow these preliminary steps.

Step 1: Make sure computers meet minimum requirements

Important If you have clients using earlier versions of Macintosh Manager, be sure to upgrade them to Macintosh Manager 2.2 before you connect them to the Mac OS X Server.

Client Computer Requirements

Software

- Mac OS 8.1 to Mac OS 9.x as the primary operating system
- Appearance control panel v. 1.0.1 or later

Note: Macintosh Manager is not used to manage Mac OS X clients.

Hardware

- Macintosh computer with a 68K processor
- 8 megabytes (MB) of physical random access memory (RAM) (not virtual memory)
- 2 MB of disk space available

- 16-bit monitor recommended if using the Panels environment

Administrator Computer Requirements

Software

- Mac OS X Server (with Macintosh Manager administrator software) installed
You can also install only the Macintosh Manager administrator software if you want to access the administrator software on a nonserver computer (the computer must use either Mac OS X v10.2 or Mac OS 9.2 as the operating system).

Hardware

- Macintosh computer with a G3 processor
- 128 MB of RAM; at least 256 MB of RAM for high-demand servers running multiple services
- 4 gigabytes (GB) of available disk space
- Minimum monitor resolution of 800 x 600

Note: Automatic hardware restart requires a Macintosh Server G4 or Power Mac G4 released in February 2000 or later.

Step 2: Install Macintosh Manager administrator software

You can use Macintosh Manager administrator software in either Mac OS X or Mac OS 9, but you cannot use it in Mac OS 8. You can install the administrator software on a Mac OS X server, on selected “administrative” client computers, or on all client computers. Only server administrators, Macintosh Manager administrators, and workgroup administrators have access to the Macintosh Manager administrator application.

Using designated administrative computers can make it easier to change or update management settings for clients. For example, if you have a set of computers in a classroom, you could install the administrator software on the teacher’s computer and give the teacher administrative access. Then, the teacher can make immediate changes as needed, such as adding users to a workgroup or providing access to a different printer.

Because the administrator computer is used to set up Macintosh Manager, the administrator computer should have access to the same printers and applications you want to use for your client computers. This makes it easier to create lists of allowed applications and printer lists

for the clients. The administrator computer can have access to more printers and applications than clients but shouldn't have access to fewer.

Important When you make printers available to client computers, Macintosh Manager creates desktop printers for your Mac OS 9 clients. The Mac OS X version of the Macintosh Manager administrator application only creates LaserWriter desktop printers. If you need to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients.

To set up an administrative client computer:

- 1 Make sure the computer meets minimum requirements.
- 2 Make sure the system software is either Mac OS X or Mac OS 9.2.
- 3 Make sure necessary applications are installed.
- 4 Set up printer access using either Print Center (for Mac OS X) or Desktop Printer Utility (for Mac OS 9).
- 5 Install Macintosh Manager administrator and client software.

Before you use the Macintosh Manager administrator application, open the Sharing preference in System Preferences in Mac OS X and make sure Web sharing and file sharing are turned off. If you are using Mac OS 9, check the settings for the File Sharing and Web Sharing control panels.

Step 3: Set up client computers

Mac OS 9 computers and Mac OS 8 computers require different setup procedures.

To set up Mac OS 9 client computers:

- 1 Make sure the computer meets minimum requirements.
- 2 Make sure the system software is Mac OS 9 (version 9.1 or later recommended).
- 3 Install Macintosh Manager client software, if it is not already installed.
- 4 Open the Multiple Users control panel.
- 5 Click Options, then click Other.
- 6 Select "Macintosh Manager account (on network)."
- 7 Click Save.
- 8 Select "On" to turn on Multiple User Accounts.
- 9 Close the control panel, and then choose Logout from the Special menu.

The computer locates Macintosh Manager servers (any Mac OS X Server with Macintosh Manager server processes installed) on your network automatically when you log out. You can select the server you want to use. If the computer can't locate a Macintosh Manager server, browse to find the TCP/IP address (not the AppleTalk address) of the server you want.

To set up Mac OS 8 client computers:

- 1 Make sure the system software is Mac OS 8 (version 8.1 or later).
- 2 Install Macintosh Manager client software.
- 3 Restart the computer.

To stop managing Mac OS 8 client computers, remove the Multiple Users startup extension from the System Folder and restart the computer.

Important For computers using Mac OS 8.6, a user in the Finder environment can access the Startup Disk control panel. Disable the control panel with Extensions Manager before you use Macintosh Manager with those computers.

Using Update Packages

If you are already using Macintosh Manager 2.0 or later on a client computer, you can easily upgrade to the latest version of Macintosh Manager by using an automatic update package. The update package is located on the Macintosh Manager installation CD. It is not installed automatically.

To use an update package:

- Copy the update package to the Multi-User Items folder on your Macintosh Manager server.

All connected clients periodically look for an update package in the Multi-User Items folder. If an update package is found, clients run the update automatically regardless of whether or not the update is for a new or previous version. Before you use an update package, be sure to shut down any computers you don't want to update. After the update is complete, remove the update package from the Multi-User Items folder, and then restart the client computers.

Choosing a Language for Macintosh Manager Servers and Clients

Ideally, the language used on client computers should match the language used on the Macintosh Manager server. However, if you want to set up different languages on certain client computers, you can do so.

Client computers using different languages can connect to the same server provided the server language script matches the client language script. For example, a user at a client computer that uses French-language client software with the script set to Roman can connect to the server. Another user at a German client computer using Roman script can also use the same server. You can set the script in the International pane of System Preferences (in Mac OS X) or using the International control panel (in Mac OS 9 or 8).

When a user connects to a Macintosh Manager server, the client computer should use the same language software that was used during any previous connections. For example, if a user connects to the Macintosh Manager server from a French client computer and then from a German client computer, preference folders and other folders in the user's home directory may be created for each language, so the user may not be able to share preferences across languages. On the other hand, if separate folders are not created, then different-language versions of two programs may end up sharing a preference file. This could cause the client computer to freeze.

Changing the Apple File Service Language Script

The correct Apple file service language script (for “Encoding for older clients”) should be selected before using the Macintosh Manager server. If Macintosh Manager service is already in use, stop Macintosh Manager service before changing the language script.

The “Encoding for older clients” script should match the client computer's language script (selected in the International pane of System Preferences) in addition to the language script used for the Macintosh Manager administration application.

Step 4: Make sure you've set up users and their home directories

If you haven't set up users and home directories already, do so before you proceed. Read Chapter 3, “Users and Groups,” for more information.

Inside Macintosh Manager

The sections that follow describe some of Macintosh Manager's components and provide background information about how Macintosh Manager works with other Mac OS X Server services.

Macintosh Manager Security

Although Macintosh Manager is not a designated “security application,” you can use Macintosh Manager settings to provide more administrative control or to allow greater flexibility for users. For example, you might want to restrict local file and system access privileges, allow users to play audio CDs, or allow users to access some applications but not others.

Macintosh Manager users cannot access other users' home directories, nor can they change network settings (AppleTalk and TCP/IP control panels), Energy Saver settings, or Multiple Users settings.

Macintosh Manager's design prevents users from renaming Macintosh Manager files or changing the file type or creator. In addition, the Macintosh Manager extension is not affected if a computer is restarted with extensions off, and users cannot disable the Macintosh Manager extension by moving it or turning it off.

About the Macintosh Manager Share Point

When Macintosh Manager server software is installed, a share point named Macintosh Manager is created on the server. Its permissions are automatically set to allow access from Macintosh Manager. Users who don't have administrative privileges can't see the contents of the share point and do not interact with it. The Macintosh Manager share point exists primarily to service the databases, but it is also the default location for the workgroup document volume. For more information about the contents of the workgroup document volume, see "Sharing Information in Macintosh Manager" on page 443.

If you need to save space, 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. Avoid using non-ASCII special characters (such as •, å, é, or ü) or any double-byte characters (such as Kanji characters) in the names of share points you plan to use with Macintosh Manager.

Important Do not place the Macintosh Manager share point on a UFS-formatted volume.

The Multi-User Items Folder

The Multi-User Items folder is located in the Macintosh Manager share point. Files and folders inside the Multi-User Items folder contain information about options 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 items:

- *Activity Log file*: This file contains log entries used to generate reports that show information such as login activity, printer usage, and application usage. You can define the number of entries in the Activity Log file. See "Setting the Number of Items in a Report" on page 463 for more information.
- *CD-ROM Preferences file*: This file contains a list of CDs users are allowed to use, along with any settings for specific items on each CD.
- *Computers folder*: This folder contains database files that store Macintosh Manager settings for each computer list you set up.

- *Groups folder:* This folder contains a folder for each Macintosh Manager workgroup and database files that store information about Macintosh Manager settings for each workgroup, such as the allowed items list and the location of the workgroup document folder.
- *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 created again the next time you use Macintosh Manager.
- *Printers folder:* 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 Macintosh Manager workgroup. When a user logs in to a workgroup that uses a desktop printer, the printer information 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 folder:* 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.

How the Multi-User Items Folder Is Updated

The client's Multi-User Items folder is always updated when you make changes in Macintosh Manager. A copy of this folder is stored automatically in the System Folder of each client computer. If the client computer's Multi-User Items folder is deleted, the computer downloads a new, clean copy from the server as needed, but not while a user is logged in. The folder is also updated under the following circumstances:

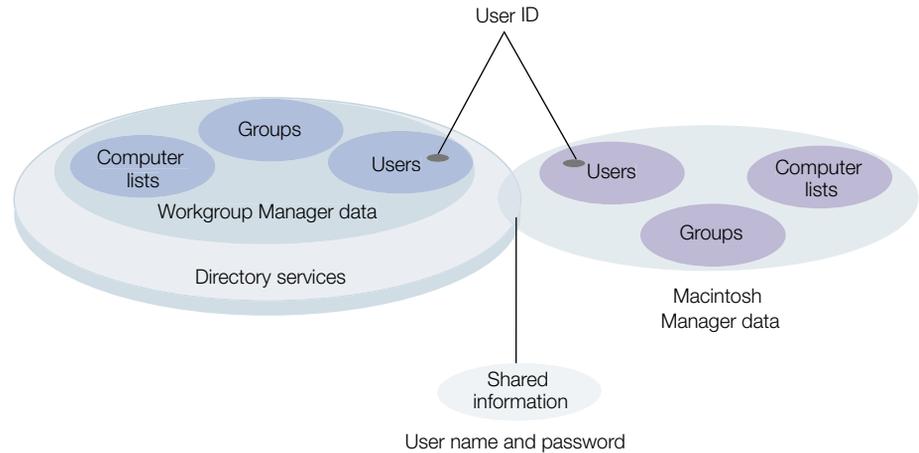
- If a client computer is connected to the server, but no users are logged in, Macintosh Manager checks periodically to see if any items in the folder need to be updated. If changes were made while a user is logged in to a computer, the folder isn't updated until the user logs out.
- If a computer is 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.
- If the client's Multi-User Items folder is deleted, the client downloads a new, clean copy from the server when a user logs in.

How Macintosh Manager Works With Directory Services

Both Macintosh Manager and Workgroup Manager have access to user account information in the Directory Services database. If you are managing Mac OS 9 or Mac OS 8 clients, you must import users from Workgroup Manager into Macintosh Manager or use Macintosh Manager's All Other Users feature in order to provide user access to your managed network.

The only information shared between Macintosh Manager and Workgroup Manager is the user ID, which is stored in Directory Services along with the user name, password, and information about the location of the user’s home directory.

For more information about Directory Services, see Chapter 2, “Directory Services.”



Macintosh Manager uses the user ID to verify and obtain a user’s user name and password through Directory Services and to find the user’s home directory. The user ID is also used to match users to the correct workgroups, preferences, and computer lists in Macintosh Manager. All other user information, such as user storage quotas and system access privileges, is set up using Macintosh Manager. After users are imported, you can create workgroups for those users and create lists specifying which computers your workgroups can use. Macintosh Manager workgroups and computer lists are completely independent of Workgroup Manager groups and computer lists.

Where User Information Is Stored

Macintosh Manager stores information about settings for users, workgroups, and computers in database files located in folders inside the Multi-User Items folder. The User, Group, and Computers folders each contain two database files:

- One file contains an index of each record in the database (such as the name of a workgroup).
- 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 to which a user belongs. To maintain consistency between databases, Macintosh Manager checks references from one database to another and updates the databases as needed.

How Macintosh Manager Works With Home Directories

You can set up home directory locations when you create user accounts. If a user doesn't have a home directory, he or she will not be able to log in. Mac OS 9 and Mac OS 8 managed clients mount the user's home directory automatically when a user logs in. The user is the owner of his or her own home directory and has full access to its contents. Macintosh Manager prevents access to other users' home directories, even if the folder's permissions have been set to allow access.

For more information about creating user accounts and home directories, see Chapter 3, "Users and Groups."

How Macintosh Manager Works With Preferences

In addition to controlling certain privileges, Macintosh Manager allows you to control application preferences and System Preferences. You can define these preferences using folders inside a user's Managed Preferences folder.

- Preferences in the Initial Preferences folder are set only once for a user.
- Preferences in the Forced Preferences folder are set every time a user logs in.
- To control preferences for Mac OS 8 users, you can use the Preserved Preferences folder.

For more information about how to use these folders to control user preferences, see "Managing Preferences" on page 466.

Where Macintosh Manager Preferences Are Stored

This section describes how user-specific preferences (such as Web browser "favorites" and desktop backgrounds) are stored in a Macintosh Manager environment. There are some differences in how preferences are handled on Mac OS 9 and Mac OS 8 computers.

Macintosh Manager stores and accesses preferences this way:

- *When a user is not logged in:* Most of a user's individual preferences are stored on the server, for both Mac OS 9 and Mac OS 8 client computers.
- *When a 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 varies depending on which operating system is used:

For Mac OS 9 clients: Preferences are stored in the /Library/Classic/Preferences folder in the user's home directory.

For Mac OS 8 clients: Preferences are stored in the Preferences folder in the System Folder on the client computer's hard disk.

If a user does not have a home directory, you can store preferences for Mac OS 9 in the Preferences folder in the Users folder on the client hard disk, but you cannot store them in the Preferences folder in the System Folder.

Using the MMLocalPrefs Extension

If some applications create excess network activity, storing preferences locally may help decrease the overall burden on your network. You can install the MMLocalPrefs extension on Mac OS 9 computers to allow Macintosh Manager to store and access user preferences locally. Using the MMLocalPrefs extension may increase login and logout times because user preferences need to be copied to and from the local hard disk.

The MMLocalPrefs extension must be installed manually on individual computers, and it affects any user who can access those computers. This extension does not work on Mac OS 8 computers.

Important Do not install the MMLocalPrefs extension if you need to enable the Check Out feature for Mac OS 9 clients.

Using NetBoot With Macintosh Manager

Although you are not required to use NetBoot with Macintosh Manager, you can use it to administer each computer's system setup in labs and classrooms. With NetBoot you can provide students with identical user environments and easy access to the same resources on a secure network that is easy to maintain.

Preparation for Using NetBoot

If client computers use system software supplied by a 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 restart. Network computers are easy to maintain because the user applications need to be installed only on a disk image stored on the server.

You must 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.

The steps below give a general description of how to prepare your managed network and clients for use with NetBoot. See Chapter 12, "NetBoot," for more detailed information.

- Set up the client computers to start up from the Mac OS disk image on the server.
- Use Macintosh Manager to control user environment, preferences, and access to local and network resources.

- Install the Macintosh Manager server software on the server containing the Mac OS image that NetBoot client computers will use to start up. Use the same server to store users' documents and applications.
- Set up workgroup administrator accounts for certain users, such as teachers or technical staff, then show them how to use Macintosh Manager to manage user accounts and workgroups.

Setting Up Mac OS 9 or Mac OS 8 Managed Clients

The following steps provide an overview of the initial setup process for managing clients in Macintosh Manager. Detailed information and tasks related to each part of the process are contained in other sections of this chapter as indicated by page references.

Step 1: Make sure Macintosh Manager services are available

In the General pane of Server Settings, click the Macintosh Manager service icon. If Macintosh Manager is available, you will see a globe on the service icon and the first menu item will be Stop Macintosh Management service. If the first menu item is Start Macintosh Management Service, choose it to start Macintosh Manager.

Step 2: Log in to Macintosh Manager Admin as an administrator

For instructions, see “Logging In to Macintosh Manager as an Administrator” on page 425.

Step 3: Import user accounts

You can import user accounts from Workgroup Manager or from a text file, and you can use a template to apply settings. Macintosh Manager provides a Guest User account. You can also use the All Other Users account to provide access to unimported users.

For more information about working with user accounts, see “Importing User Accounts” on page 426.

Step 4: Designate a Macintosh Manager administrator

For instructions, see “Designating Administrators” on page 431.

Step 5: Designate workgroup administrators

For instructions, see “Designating Administrators” on page 431.

Step 6: Create workgroups for users

Workgroups let you group users together and apply the same settings to all the users. You can set up workgroups according to any criteria, such as purpose (video production) or location (a fourth-grade classroom), and provide users with convenient access to necessary resources. You can also use a template to apply workgroup settings.

For more information about creating workgroups, see “Setting Up Workgroups” on page 436.

Step 7: Create computer lists

Computer lists let you group computers and apply the same settings to all the computers. You can use a template to apply settings to a computer list. The All Other Computers account lets you provide managed network access to computers that aren't in a computer list.

For more information about using computer lists, see “Setting Up Computer Lists” on page 451.

Step 8: Select global settings and set up managed preferences folders

In addition to various settings for users, workgroups, and computers, Macintosh Manager provides other security and CD-ROM settings in the Global pane. You can also manage user preferences by placing preference files in Forced, Initial, or Preserved preferences folders.

For information about using global settings, see “Using Global Security Settings” on page 462 and “Using Global CD-ROM Settings” on page 465.

For information about using managed preference folders, see “Managing Preferences” on page 466.

Logging In to Macintosh Manager as an Administrator

The first time you open the Macintosh Manager administrative software and log in, you can use your Mac OS X Server administrator account. Later on, you can still log in to Macintosh Manager Admin using that account or other Macintosh Manager administrator accounts that you set up.

To log in to Macintosh Manager:

- 1** Click the Macintosh Manager icon in the Dock to open Macintosh Manager. To open Macintosh Manager from Workgroup Manager, click the Macintosh Mgr icon and select Open Macintosh Manager.
- 2** Enter your Mac OS X Server administrator account user name and password.

After you log in, you can add user accounts, create workgroups, create computer lists, designate administrators, and access and change Macintosh Management service settings.

Working With Macintosh Manager Preferences

Macintosh Manager preference settings let you choose a sorting method for users and workgroups and choose a format for exported reports. Only Macintosh Manager administrators can change these settings.

To change Macintosh Manager preferences:

- 1 Log in to Macintosh Manager.
- 2 Choose Preferences from the Macintosh Manager menu (in Mac OS X) or choose Preferences from the File menu (in Mac OS 9).
- 3 Select settings for sorting users (by either name or type).
- 4 Select settings for sorting workgroups (by either name or environment).
- 5 Select a format for reports exported to a text file (using either tabs or commas to separate information fields).
- 6 If you want to use templates for users, groups, or computers, select “Show template” to include the “template” item in the list of accounts.

Importing User Accounts

This section explains various ways to import users and apply user settings. All user accounts must be created before you can import or modify them using Macintosh Manager. You cannot create user accounts in Macintosh Manager. If you have not already set up users, see Chapter 3, “Users and Groups,” for information and instructions.

Macintosh Manager user accounts are for anyone who uses a computer in a managed environment. Most users do not require access to the Macintosh Manager administrator application. If you want to give certain users (for example, managers, teachers, and so forth) administrative privileges, read “Designating Administrators” on page 431 for details.

You select user settings and user type in the Users pane of Macintosh Manager. You can select options manually or use a template to apply settings as users are imported.

Applying User Settings With a Template

You can create a template and use it to apply identical settings to multiple users at once during import. This makes it easy to start managing large numbers of users quickly.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To set up or change a user template:

- 1 In the Users pane of Macintosh Manager, select Template in the Imported Users list.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

- 2 In the Basic and Advanced panes, set options you want to use for the template, then click Save.

Importing All Users

If you have a small number of users in your Mac OS X Server database, you may want to import them to Macintosh Manager all at once. You can import up to 10,000 users with the Import All feature.

To import all users:

- 1 In Macintosh Manager, click Users.
- 2 Click Import All.

An individual Macintosh Manager user account is created for each imported user. Depending on the number of users imported, this process may take some time. You can also import users individually or in groups.

If you have more than 10,000 users to import, you may want to consider importing users from a text file.

Importing One or More Users

If necessary, you can import individual users or small groups of users. You must be using Macintosh Manager Admin in Mac OS X in order to import one user at a time. You cannot import one user at a time using Macintosh Manager on a Mac OS 9 computer.

To add one or more users to Macintosh Manager:

- 1 In Macintosh Manager, click Users.
- 2 Click Import.
- 3 If Workgroup Manager is not already open, a message about adding users appears. Click Open to open Workgroup Manager.
- 4 In Workgroup Manager, click Users & Groups, then select Show Users & Groups List.
- 5 In the Users & Groups List, select the user or users you want to import, then drag them to the Imported Users list in Macintosh Manager. You may need to rearrange the windows so that you can see both lists.

If you can't find a user in the Users & Groups List, that user may not be in your Mac OS X Server directory.

If you have fewer than 10,000 users to import, you can also use the Import All feature.

Collecting User Information in a Text File

You can create a plain text file that contains user information and then use this file when you import users into Macintosh Manager. Your file must contain at least one of the following pieces of information about each user: user ID, user name, or short name. You do not need to list password information.

To collect user information in a text file:

- 1 Make sure each user in the file already exists in directory services. Information for missing users is ignored.
- 2 Make sure each line of user information is separated by a hard return.

If you have multiple items of user information on each line, make sure the items are separated by either commas or tabs.

- 3 Make sure the file is saved as plain text and has “.txt” at the end of the file name.

To reduce the likelihood of error, avoid mixing types of user information in the text file. For example, you could use only the user ID for each user.

Importing a List of Users From a Text File

Using a text file to import user information is a convenient way to start managing large numbers of users.

To import users from a text file:

- 1 In Macintosh Manager, click Users.
- 2 Choose Import User List from the File menu, then select the file you want to import.
- 3 In the Available Fields list, select the list item that matches the first item of user information in your text file, then click Add to add the item to the Import list.

For example, if the first item in your text file is the user ID, the first item you add to the Import list should be user ID. Do the same for other information you want to import.

- 4 Choose either tab or comma for the field delimiter, depending on how you separated pieces of user information in your text file.
- 5 Click Open Sample Import to preview imported information, or click OK to start the import.

If a user cannot be found, you will see a warning message. Users in the text file must be present in the directory services database before you can import them into Macintosh Manager.

Finding Specific Imported Users

You can use the “Select Users By” feature to search for Macintosh Manager users according to chosen criteria.

To search for users:

- 1 Open Macintosh Manager, then click Users.
- 2 If “Template” appears in the list of users, make sure it is not selected.
- 3 Choose Select Users By from the Edit menu.
- 4 Select the kinds of search information you want to use.

If you select Comment, you can find users that have certain words in their comment fields.

Providing Quick Access to Unimported Users

If you want to allow user access to a managed network without having to set up user accounts, you can use the All Other Users feature, or you can set up a guest user account.

If mobile clients require access to your network, you may also want to use the All Other Computers account.

Using Guest Accounts

In Macintosh Manager, you can create three types of “guest” accounts, all of which can be managed.

■ All Other Users

Using All Other Users is a quick way to provide access to large numbers of users and manage them without having to import them into Macintosh Manager. Users with existing Mac OS X user accounts can log in and access their own home directories, preferences, and documents. They have the privileges and environment you set up for the All Other Users Account. You can also set login settings for All Other Users and allow them to exceed printer quotas.

For information about how to set up the All Other Users account see “Providing Access to Unimported Mac OS X Server Users” on page 430.

■ Guest Users

When a user logs in as Guest, no password is required. Anyone can use the guest account when it is available, whether he or she has a Macintosh Manager user account, a Mac OS X Server user account, or no account at all.

All users logged in as Guest have the same privileges and preferences. Any settings you choose for the guest account apply to all users who log in as Guest. You can set login settings and user storage quotas for guest users. You can also allow them to exceed printer quotas.

For more information about using the guest user account, see “Setting Up a Guest User Account” on page 431.

- All Other Computers

Any computer that is “unknown” or not in a Macintosh Manager computer list uses settings selected for the All Other Computers account. Allowing unknown or “guest” computers is useful if you want to manage users who want to connect to your network using their own portable computers.

For more information about how to set up the All Other Computers account, see “Setting Up the All Other Computers Account” on page 452.

Providing Access to Unimported Mac OS X Server Users

After you enable the All Other Users feature, Macintosh Manager creates the All Other Users account and makes it available in the Imported Users list. You can treat the All Other Users account like any other user account with its own workgroup and settings, with a few exceptions:

- Computer checkout is not allowed.
- Working offline at a client computer is not allowed.
- A disk quota is not enforced.

Using the All Other Users account is the quickest and most convenient way to grant authenticated access and set up customized environments for users without having to import them into Macintosh Manager. For example, in a school with a central user database, you can set up Macintosh Manager service in a computer lab using only the All Other Users account. Any user on campus who has a Mac OS X Server account can walk into the lab, log in, and access his or her home directory in a managed environment.

To set up the All Other Users account:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 Select Allow “All Other Users” and click Save.
- 3 Click the Users tab and select All Other Users in the Imported Users list.
- 4 Select settings in the Basic and Advanced panes, then click Save.
- 5 Click Workgroups, add All Other Users to a workgroup, and give the workgroup a name.
- 6 Select settings for that workgroup, then click Save.
- 7 Click Computers and make computers available to the workgroup you just created.

Setting Up a Guest User Account

Because the Guest account does not require individual user names and passwords for each user, it is a good choice for setting up a public computer or kiosk where users do not need to access their home directories.

After you enable the Guest account, Macintosh Manager creates the account and makes it available in the Imported Users list. As with any other user account, you can add the Guest account to a workgroup and apply Macintosh Manager settings, with a few exceptions:

- Computer checkout is not allowed.
- Working offline at a client computer is not allowed.

To set up the Guest account:

- 1 Open Macintosh Manager, click Global, and then click Security.
- 2 Select “Allow Guest access.”
- 3 Click Users, and select Guest from the Imported Users list. In the Basic and Advanced panes, select the settings you want to use.
- 4 Click Workgroups. Create a workgroup for the Guest account, or select an existing workgroup and add Guest to the Workgroup Members list in the Members pane.
- 5 Provide access to computers by making one or more lists of computers available to the workgroups.
- 6 Click Save.

Designating Administrators

After you import user accounts, you'll need to give some users administrative privileges. For Macintosh Manager, the privilege hierarchy is similar to that of Workgroup Manager, but Macintosh Manager uses only two types of administrative accounts. Macintosh Manager workgroup administrators are similar to Workgroup Manager's directory domain administrators, but their privileges apply only to workgroups created in Macintosh Manager.

About Macintosh Manager Administrators

A Macintosh Manager administrator can import, edit, and delete user accounts and create workgroup administrators and additional Macintosh Manager administrators. A Macintosh Manager administrator can change any of the Macintosh Manager settings and, if allowed, can use his or her administrator password to log in as any user except another Macintosh Manager administrator.

A Macintosh Manager administrator's administrative privileges do not apply in Mac OS X Workgroup Manager tools. For example, a Macintosh Manager administrator cannot create user accounts in Workgroup Manager (unless he or she also has a Mac OS X server administrator account).

Allowing Mac OS X Server Administrators to Use Macintosh Manager Accounts

Because Macintosh Manager is disconnected from data (other than the user ID) used by Workgroup Manager, Mac OS X Server administrator accounts are imported to Macintosh Manager as regular users. They may not be able to access their home directories when they log in to client computers, and they will not automatically have administrative privileges in Macintosh Manager. They cannot access the Macintosh Manager share point or set up managed preferences.

You should create a separate Mac OS X Server user account for any server administrators you want to include in Macintosh Manager, and then import those accounts. If you want to give these users full administrative privileges in Macintosh Manager, follow the instructions for “Creating a Macintosh Manager Administrator” on page 432.

About Workgroup Administrators

Workgroup administrators can add or modify user accounts and workgroups according to privileges assigned to them. Regardless of privileges, they cannot change a user's type or change access settings, and they cannot create Finder workgroups.

Workgroup administrators also have access to shared folders, such as hand-in folders, which can be used to collect documents from users. In a school environment, for example, teachers who are workgroup administrators can distribute and collect assignments over the network. A teacher can also make available various network resources, applications, and CDs that promote teaching objectives for the class.

Creating a Macintosh Manager Administrator

You should create at least one Macintosh Manager administrator to prevent users from bypassing security and changing to a different Macintosh Manager server.

To designate a Macintosh Manager administrator:

- 1 In Macintosh Manager, click Users.
- 2 Select one or more users in the Imported Users list.
- 3 Change the user type to Macintosh Manager Administrator, then click Save.

Creating a Workgroup Administrator

You can set up workgroup administrator accounts for people (such as teachers or technical coordinators) who may need to add or modify certain user accounts or workgroups.

To designate a workgroup administrator:

- 1 In Macintosh Manager, click Users.
- 2 Select one or more users in the Imported Users list.
- 3 Change the User Type to Workgroup Administrator, then click Save.

Changing Your Macintosh Manager Administrator Password

Macintosh Manager administrators can change their passwords whenever necessary.

To change your administrator password:

- 1 Log in to Macintosh Manager.
- 2 Choose Change Password from the Configure menu.
- 3 In the text fields provided, type your current password, then type your new password. Then, type your new password again to verify it.

Working With User Settings

This section describes basic and advanced user settings and how to use them. Available settings in the Advanced pane vary depending upon the user type. All users have the same options available for basic settings regardless of user type.

Changing Basic User Settings

Name, short name, and ID information is imported with each user. This information cannot be changed in Macintosh Manager. For information about how to change this information, see Chapter 3, “Users and Groups.”

You can change basic settings for more than one user at a time. When you have multiple users selected, the name, short name, and ID change to “Varies.”

To change Basic user settings:

- 1 In Macintosh Manager, click Users, and then click Basic.
- 2 Select one or more users in the Imported Users list.
- 3 Select a type from the User Type pop-up menu.
- 4 Select login settings.

“User can log in” is already selected for you. Deselect it if you want to disable user login immediately.

If you want to prevent a user from logging in after a specific date (for example, after a school session ends), select “Disable log-in as of ___” and type in a date.
- 5 Add comments (up to 63 characters long) in the Comments field.

This is a good place to put user-specific information (for example, a student's grade level or an employee's office location) or keywords that will help you find users.

- 6 Click Save.

Allowing Multiple Logins for Users

Ordinarily, users must log out on one computer before they can log in on another. However, you may want to allow certain users, such as technical support staff or administrators, to log in on several computers simultaneously (to do maintenance tasks, for example).

To allow simultaneous logins:

- 1 In Macintosh Manager, click Users, and then click Advanced.
- 2 Select a user from the Imported Users list.
- 3 Deselect "User can only log in at one computer at a time."
- 4 Click Save.

Granting a User System Access

Users who have system access can access all items on a client computer, including the Finder and the System Folder. Grant system access to specific users, such as workgroup administrators or technical support staff, only if necessary. Macintosh Manager administrators always have system access.

To allow system access for a user:

- 1 In Macintosh Manager, click Users, and then click Advanced.
- 2 Select a regular user or workgroup administrator in the Imported Users list.
- 3 Select "User has system access."
- 4 Click Save.

Changing Advanced Settings

Depending upon the user type, some advanced settings may or may not be available. Also, workgroup administrators cannot change access settings, email settings, or user type.

To change advanced settings for a user:

- 1 In Macintosh Manager, click Users, and then click Advanced.
- 2 Select the user or users you want to modify in the Imported Users list.

You can select multiple users, but they should be of the same type. If you select different types of users, you will be able to modify only the advanced settings that those users have in common.

- 3 Select access settings and set quotas.

Initially, users of all types can log in to only one computer at a time. No other settings are selected.

- 4 If the user is a workgroup administrator, select the privileges you want the user to have under “Allow this Workgroup Administrator to.” Initially, no privileges are selected.
- 5 Click Save.

Limiting a User’s Disk Storage Space

A disk space quota limits the amount of storage space available in a user’s home directory. Once a user exceeds the storage limit, he or she cannot save any more files there. Users see a warning message if they run out of storage space.

To set a user storage quota:

- 1 In Macintosh Manager, click Users, and then click Advanced.
- 2 Select a user in the Imported Users list.
- 3 Select “Set user storage quota to ___ K” and type in the maximum amount of storage space to allow in kilobytes (1024 kilobytes = 1 megabyte).

When you set a storage quota, keep in mind the amount of space available and the number of users who will share it.

- 4 To allow a user to save files even if he or she exceeds the set quota, select “Only warn user if they exceed this limit.”
- 5 Click Save.

Updating User Information From Mac OS X Server

If you change user information in Workgroup Manager or delete user accounts, you need to synchronize Macintosh Manager with the Mac OS X Server database to make sure user data is the same in both places.

To update Macintosh Manager user data:

- 1 In Macintosh Manager, click Users.
- 2 Choose Verify Users & Workgroups from the File menu.

If the user account exists in the server database, Macintosh Manager updates the user’s information to match information in the server database. For very large numbers of users, this process can take some time.

Note: If the user account can’t be found, the user is deleted from Macintosh Manager.

Setting Up Workgroups

In the Members pane of the Workgroups pane, you can create new workgroups, change an existing workgroup's name or type, and add or remove workgroup members.

Important If a user is not a workgroup member, he or she cannot log in to the Macintosh Manager network. Group accounts are not imported from Workgroup Manager; you must create them. Every managed user must belong to at least one workgroup. Users can belong to more than one workgroup, but users can select only one workgroup when they log in.

This section describes the different workgroup environments and tells you how to apply workgroup settings manually, by duplicating a workgroup, and by using a template.

Types of Workgroup Environments

Workgroups can have one of three types of desktop environments. All three types have some optional settings in common. Important differences are described below.

- Finder workgroups have the standard Mac OS desktop.
The System Folder and Applications folder are not automatically protected, but you can choose to protect them. Members of Finder workgroups have no restrictions on the File menu, Apple menu, or Special menu. They also have no restrictions on removable media or CDs.
- Restricted Finder workgroups have the standard Mac OS desktop, but with restrictions.
The System Folder and the Applications folder are protected. This means users can view the contents, but cannot modify them or add new items. Users can access File menu and Special menu items, but you can choose available items for the Apple menu. You can also control the user's ability to take screen shots, and you can choose privileges for CDs, removable media, and shared folders.
- Panels workgroups have a simplified interface with large icons that make using a computer easy for novice users, particularly children.
Panels workgroup options are the same as Restricted Finder options, with a few additions. You can control access to the File menu and the Special menu in addition to the Apple menu, and you can select whether or not to show a mounted volume as a panel. Members of a Panels workgroup cannot view items on the local hard disk.

Creating a Workgroup

Workgroup members can be of any user type, and workgroups can have up to 1500 members. Workgroup administrators, if allowed, can create Restricted Finder and Panels workgroups, but they cannot create Finder workgroups.

To create a workgroup:

- 1 In Macintosh Manager, click Workgroups.

- 2 Click New and type a name for the workgroup.
- 3 Choose an environment type from the Environment pop-up menu.
- 4 Select one or more users in the Available Users list and click Add.
To remove workgroup members, select the users you want to remove in the Workgroup Members list, then click Remove.
- 5 Choose settings for this workgroup in the other panes, then click Save.
You can duplicate workgroups or use a template to apply settings to new workgroups.

Using a Template to Apply Workgroup Settings

You can use a template to quickly create several workgroups that have the same settings. Once you modify the template, each new workgroup you create will have the template settings. You can make additional changes to the workgroup after it is created.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To set up or change a template:

- 1 In Macintosh Manager, click Workgroups.
- 2 Select Template in the Workgroups list.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

- 3 In each of the Workgroup panes, set the options you want to use in the template, then click Save.

Creating Workgroups From an Existing Workgroup

Duplicating an existing workgroup is a quick way to create another Macintosh Manager workgroup that already has settings or members you want.

To duplicate a workgroup:

- 1 In Macintosh Manager, click Workgroups. Then select a workgroup in the Workgroups list.
- 2 Click Duplicate and type a new name for the workgroup.
- 3 Add or remove members and change settings if you wish, then click Save.

Modifying an Existing Workgroup

After a workgroup is created, you can change its name or environment type and add or remove members. A workgroup administrator can change settings for a workgroup only if he or she is also a member of that workgroup.

To change Members settings:

- 1 In Macintosh Manager, click Workgroups, and then click Members.
- 2 Change the workgroup name in the text field.
- 3 Select a new environment in the pop-up menu.

Workgroup administrators cannot select Finder as a workgroup environment.

- 4 To add new members, select one or more users in the Available Users list and click Add. To remove members, select members in the Workgroup Members list, and click Remove.
- 5 Click Save.

Using Items Settings

Items settings let you make files and applications on client computers available to workgroup members.

Setting Up Shortcuts to Items for Finder Workgroups

You can use settings in the Items pane to create a list of applications, folders, and files that workgroups can access. If you choose to allow access to local items, the items appear in the Shortcut Items list. Macintosh Manager creates an alias for each item in the list.

Aliases for shortcut items appear on the user's desktop. When users log in, their computers look for the original file at the "Find chosen items" location and create an alias for the file.

Important Unless you plan to look for original items only on local volumes, be sure personal file sharing is turned off and other Apple Filing Protocol (AFP) services are not running before you proceed. Alternatively, use a computer that has Macintosh Manager, but not file service, installed.

To make items on the local volume available to a workgroup:

- 1 In Macintosh Manager, click Workgroups, and then click Items.
- 2 Select "Members can open any items on local volumes" if you want to allow access to items stored on the computer where users are logged in.

If you select this option, access is not restricted, but you can use Shortcut Items to provide quick access to a particular set of applications, folders, and/or files.
- 3 Select a volume in the Volume pop-up menu.

- 4 Select items in the Volume list that you want to add to the Shortcut Items list and click Add.
To remove items from the Shortcut Items list, select them and click Remove. Use Find to search for additional items, such as files or folders.
- 5 Select a location from the “Find chosen items” pop-up menu.
A user’s computer looks for the original file at this location, and then downloads the alias.
- 6 Click Save.

Making Items Available to Panels or Restricted Finder Workgroups

If you choose to allow access to only specific items, the items appear in the Approved Items list. Macintosh Manager creates an alias for each item in the list.

Aliases for approved items appear either on a panel for Panels workgroups or in a folder on the desktop for Restricted Finder workgroups. When users log in, their computers look for the original file at the “Find chosen items” location and create an alias for the file.

Important Unless you plan to look for original items only on local volumes, be sure personal file sharing is turned off and other AFP services are not running before you proceed. Alternatively, use a computer that has Macintosh Manager, but not file service, installed.

To provide access to applications and other items:

- 1 In Macintosh Manager, click Workgroups, and then click Items.
- 2 Select an application access setting.
Select “Members can open any items on local volumes” if you want to allow access to items stored on the computer where users are logged in. If you select this option, access is not restricted, but you can use Shortcut Items to provide quick access to a particular set of applications, folders, and/or files.
Select “Allow members to open only the following items” if you want to allow access to only certain approved applications, folders, or files.
- 3 Select a volume in the Volume pop-up menu.
- 4 Select items in the Volume list that you want to add to the Approved Items or Shortcut Items list, and click Add. You can also drag and drop items directly into the list.
To remove items from the list, select them and click Remove. Use Find to search for additional items, such as files or folders.
- 5 Select a location from the “Find chosen items” pop-up menu.
When a user attempts to open a Shortcut Items or Approved Items alias, the computer looks for the original file at the “Find chosen items” location.

The computer can search local volumes and mounted server volumes. If the original item is on a server volume that is not mounted, the computer won't be able to find it.

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.

- 6 Click Save.

Making Items Available to Individual Users

In some cases, you may want to make specific documents or applications available to individual users. For example, a user working on a special video project may require a video-editing application that other workgroup members don't need.

To make items available to a specific user:

- Place the items in the user's home directory.

Using Privileges Settings

Settings in the Privileges pane allow you to enable certain security measures, control access privileges for workgroup folders, and set options to allow users to take screen shots, play audio CDs, and open items on removable media. Available privilege settings vary depending upon the type of workgroup selected in the Workgroups list. If you have more than one type of workgroup selected when you make changes, you will be able to change only those settings that the workgroups have in common.

Protecting the System Folder and Applications Folder

For Panels and Restricted Finder workgroups, these folders are always locked. Users can view the contents, but cannot make changes. Finder workgroups do not automatically have these folders protected, but you can set these restrictions.

To protect these folders:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Finder workgroup in the Workgroups list.
- 3 Click the checkboxes next to System Folder and Applications folder to protect them.
- 4 Click Save.

Protecting the User's Desktop

You can prevent users from storing files or folders on the desktop and changing the desktop pattern, icon arrangement, or other desktop settings.

To protect the desktop:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a workgroup in the Workgroups list.
- 3 Click the checkbox to select “Lock the user’s desktop on the startup volume.”
- 4 Click Save.

Preventing Applications From Altering Files

Enforcing file-level security prevents applications from writing to protected folders and files, but it may cause some older applications to report disk errors or have problems opening. If you don’t enforce file-level security, applications can write information (for example, temporary data or preferences) wherever necessary.

File-level security is available only for Mac OS 9 clients and applies only to applications. It does not affect user access to folders and files.

To enable file-level security:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a workgroup in the Workgroups list.
- 3 Select “Enable file level security for Mac OS 9 workstations,” then click Save.

Preventing Access to FireWire Disks

You can enable file-level security to prevent users in a Panels workgroup from accessing FireWire hard disks that are mounted at startup. This applies only to Mac OS 9 clients and does not affect Finder or Restricted Finder workgroups.

Allowing Users to Play Audio CDs

Users in a Finder workgroup can always play audio CDs. Panels or Restricted Finder workgroups don’t automatically have that privilege, but you can give it to them.

To allow users to play audio CDs:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Panels or Restricted Finder workgroup in the Workgroups list.
- 3 Select “Play audio CDs,” then click Save.

Some CDs contain more than just audio tracks. If the first track on a CD is an audio track, then it is an audio CD.

Allowing Users to Take Screen Shots

Special key combinations let users take a picture of the computer screen (called a “screen shot”) and save the picture as a file stored in the user’s Documents folder. Users in Finder workgroups are always allowed to take screen shots. Panels or Restricted Finder workgroups don’t automatically have this privilege, but you can give it to them.

To allow users to take screen shots:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Panels or Restricted Finder workgroup in the Workgroups list.
- 3 Select “Take Screen Shots,” then click Save.

If disk space is a concern, you may not want to enable this feature.

Allowing Users to Open Applications From a Disk

If you use a list of “approved items” (applications or scripts) that users can access, users in a Panels or Restricted Finder workgroup cannot open applications on removable media (for example, floppy disks) unless you allow it.

Finder workgroups do not have this restriction.

To allow users to open applications on removable media:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Panels or Restricted Finder workgroup in the Workgroups list.
- 3 Select “Open approved items on removable media,” then click Save.

Removable media include floppy disks, Zip disks, and all other types of removable media except CDs or DVDs.

You can set up a list of approved items in the Items pane of the Workgroups pane.

Setting Access Privileges for Removable Media

For Panels and Restricted Finder workgroups, you can set access privileges for removable media. Removable media include floppy disks, Zip disks, and all other types of removable media except CDs.

To set privileges for removable media, other than CDs:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Panels or Restricted Finder workgroup in the Workgroups list.
- 3 Select an access privilege setting from the pop-up menu next to “Removable media (except CDs),” then click Save.

Setting Access Privileges for Menu Items

For certain Finder menus, you can decide which menu items users can see. For Panels workgroups, you can control items in the Apple menu, File menu, and Special menu. For Restricted Finder workgroups, you can only control items in the Apple menu and the Special menu. Finder workgroups do not have these restrictions.

To set privileges for menu items:

- 1 In Macintosh Manager, click Workgroups, and then click Privileges.
- 2 Select a Panels or Restricted Finder workgroup in the Workgroups list.
- 3 Select each menu item you want workgroup members to be able to use, then click Save.

Sharing Information in Macintosh Manager

Macintosh Manager provides a number of ways to share information among users or workgroups by using different types of shared folders. Most shared folders are created inside the group documents volume. Some folders are created automatically, but others must be created by the administrator.

Types of Shared Folders

- Workgroup shared folder
Only members of a single workgroup can use this folder. A workgroup shared folder is automatically created when you set up a group documents volume.
- Global shared folder
Members of all workgroups whose workgroup folder is on the same volume can access this folder, allowing documents to be shared between workgroups. A global shared folder is automatically created when you select a group documents volume.
- Workgroup hand-in folder
Hand-in folders must be set up manually and are available only to Panels and Restricted Finder workgroups. The hand-in folder is stored on the group documents volume. At least one workgroup administrator or Macintosh Manager administrator must be a member of the workgroup to use this feature because only an administrator can see items in the hand-in 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).
- Folder on the startup disk named ____
A Macintosh Manager administrator can create a folder at the top level of the startup disk and then allow users to open items stored in that folder. This type of folder is useful for storing items that workgroup members need to access easily or frequently, such as clip art.

Folder Access Privileges

Macintosh Manager allows four levels of access privileges for workgroup folders:

Access setting	What it means
Read Only	Users can view and open items in the folder, but they cannot modify them, and they cannot “write to” the folder. For example, they cannot save a file in the folder.
Write Only	Users cannot view or open items in the folder, but they can write information to the folder. For example, they can copy a document to the folder.
Read & Write	Users have unrestricted access to the folder. They can view, open, modify, or write information to the folder.
No Privileges	Users cannot do anything at all with the folder.

Selecting Privileges for Workgroup Folders

After you create a group documents volume, you can set user access privileges (Read Only, Write Only, Read & Write, or No Privileges) for various workgroup folders.

To set access privileges for workgroup folders:

- 1 Make sure the group documents volume is already set up before you proceed.
- 2 In Macintosh Manager, click Workgroups, and then click Options.
- 3 Select a Panels or Restricted Finder workgroup.
- 4 Select an access privilege setting from the pop-up menu next to each type of folder that is available for the workgroup.
- 5 Click Save.

Setting Up a Shared Workgroup Folder

A shared workgroup folder is a convenient location where workgroup members can store and share any kind of information, depending on how file and folder access privileges are configured. For example, if you set up read-write permission for a shared group documents volume, several users can share HTML files or images for a collaborative project.

To set up a group documents folder:

- 1 Open Macintosh Manager.

Before you proceed, make sure the group documents settings in the Options pane are correct. If they are not, choose the correct group documents location and login settings, and then click Save.

- 2 Click Workgroups, then click Privileges.
- 3 Select one or more workgroups in the Workgroups list.
- 4 In the Privileges section, set “Workgroup shared folder” to Read & Write, then click Save.

If you want to prevent users from changing the documents in the workgroup shared folder, you can lock each document.

Setting Up a Hand-In Folder

A hand-in folder works like a drop box. Users can save items in the folder, but they can't see any items in the folder. Hand-in folders are very useful for collecting and protecting sensitive documents. For example, in a classroom, students can turn in homework by copying their files into the folder. Employees in a workplace can place status reports or personal reviews in a hand-in folder that only their managers can access.

Hand-in folders are available only for Panels or Restricted Finder workgroups.

To create a hand-in folder:

- 1 Open Macintosh Manager, click Workgroups, and then click Options.
Before you proceed, make sure the group documents settings in the Options pane are correct. If they are not, choose the correct group documents location and login settings, then click Save.
- 2 Click Workgroups, then click Privileges.
- 3 Select one or more Panels or Restricted Finder workgroups in the Workgroups list.
- 4 In the Privileges section, set “Workgroup hand-in folder” to Write Only, then click Save.

The hand-in folder appears as an item in the File menu for Panels workgroups. For Restricted Finder workgroups and workgroup administrators, it appears as a folder on the desktop.

Using Volumes Settings

You can use the Volumes settings for Workgroups to select which volumes are mounted when users log in and control login options for each volume. A volume is a shared folder on a file server.

Connecting to AFP Servers

Mac OS X Server supports TCP/IP network connections to Apple Filing Protocol (AFP) servers such as the Macintosh Manager server. You cannot use AppleTalk connections to AFP servers.

Providing Access to Server Volumes

If workgroup members need to use files and applications that are not stored on the Macintosh Manager server, you can mount volumes automatically when users log in.

Even if you don't set up a server volume to mount automatically, users can still connect to it if they have access to the network and have an account on (or guest access to) that server.

To connect to volumes automatically:

- 1 In Macintosh Manager, click Workgroups, and then click Volumes.
- 2 Select one or more workgroups.
- 3 Select a volume in the Volumes list, then click Add.

If you don't see the volume you want, click Find and locate the volume.

When the volume is mounted, it requests a login name and password.

- 4 Select a volume in the Mount at Log-in list and choose login settings (explained in the steps that follow).
- 5 If the volume doesn't use the same user names and passwords used by Macintosh Manager, select "Prompt user for log-in." Users must enter a valid user name and password.
- 6 If you want to grant easy access to a volume for all users, select "Log in automatically as this AFP user" and type in a valid user name and password.

This isn't as secure as requiring users to log in with their own information, because you can't control access individually or track who has logged in to the server.

You can select "Always try automatic log-in with user's name and password first" in addition to the other login settings.

If this attempt at login fails, the login method you selected under "When mounting" is used.

- 7 Select "Use AFP privileges" to use Apple Filing Protocol read and write permission settings to determine access privileges for a particular volume. Ordinarily, Macintosh Manager allows read-only access to volumes.

This setting does not apply to Finder workgroups.

- 8 If you select "Require an administrator password to unmount," users can't disconnect the volume unless they have the correct password.

This setting does not apply to Finder workgroups.

- 9 For Panels workgroups only, select "Show volume on a panel" if you want the user to see the volume icon.

If you don't select this option, the volume can only be seen in the Applications panel.

- 10 Click Save.

Using Printers Settings

Printers settings let you control access to workgroup printers and limit the number of pages printed. Some settings are available only if you select “Allow member to use only the following Desktop Printers.”

Making Printers Available to Workgroups

Before you can make a printer available to a workgroup, the printer must appear in the Available Printers list. You can add printers using Create New in the Printers pane of Workgroups, or you can add them in the Print Center application (in Mac OS X) on the Macintosh Manager server.

Note: The Mac OS X version of the Macintosh Manager administrator application only creates LaserWriter desktop printers. If you need to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients. To add printers in Mac OS 9, use the Chooser in the Apple menu.

To allow access to printers:

- 1 In Macintosh Manager, click Workgroups, and then click Printers.
- 2 Make sure “Allow members to use only the following Desktop Printers” is selected.
- 3 Select one or more printers in the Available Printers list and click Add.
- 4 When you have finished adding printers, click Save.

You cannot grant access to both the system access printer and desktop printers. If you want a workgroup to use the system access printer, log in to the System Access workgroup as an administrator and use the Chooser to select a printer. Then follow the steps above.

Setting a Default Printer

When a user prints a document, applications prefer to send the document to the default printer. If multiple printers are available, the user has the opportunity to select a different printer.

After printers have been added to the Available Printers list, you can determine how applications will know which printer to use first.

To select a default printer:

- 1 In Macintosh Manager, click Workgroups, and then click Printers.
- 2 Make sure “Allow members to use only the following Desktop Printers” is selected.
- 3 Select a printer in the Selected Printers list and click Set Default Printer.

If multiple printers are available and you select “Remember last used printer,” applications prefer to send print jobs to the last printer used, even if it isn’t the default printer. The user still has the opportunity to select a different printer.

Restricting Access to Printers

You can restrict access to a printer by removing it from the Selected Printers list or by requiring a password to use it.

To restrict access to a printer:

- 1 In Macintosh Manager, click Workgroups, and then click Printers.
- 2 Make sure “Allow members to use only the following Desktop Printers” is selected.
- 3 Select a printer in the Selected Printers list. If you want to remove the printer from the list, click Remove.
- 4 Select “Require an administrator password to print to this printer” to protect only the selected printer. To password-protect all printers in the list, select “Require an administrator password to print to any printer.”

Setting Print Quotas

A print quota limits the number of pages a user is allowed to print over a period of time. The number of pages allowed refers to the document’s page count, not to the number of pieces of paper. For example, if you print a 16-page document using a layout that shows four document pages on each printed page, you’ll use four sheets of paper; however, 16 pages are subtracted from your print quota. Pages are counted against the maximum allowance even if the printing job is not completed (for example, if there is a paper jam).

Using a print quota helps encourage users to use printing resources wisely and helps decrease waste. You can set an individual quota for each printer in the Selected Printers list.

To set a print quota for a user:

- 1 In Macintosh Manager, click Workgroups, and then click Printers.
- 2 Make sure “Allow members to use only the following Desktop Printers” is selected.
- 3 Select a printer in the Selected Printers list.
- 4 Select “Limit users to no more than ___ pages every ___ days” and enter the maximum number of pages to allow in a number of days.
- 5 Click Save.

Allowing Users to Exceed Print Quotas

When you set a print quota, the limitation applies to every user in the selected workgroup. However, you can allow certain users to ignore all print quotas.

To allow a user to exceed all print quotas:

- 1 In Macintosh Manager, click Users, and then click Advanced.
- 2 Select a user from the Imported Users list, then select “Allow user to exceed print quotas.”

- 3 Click Save.

Setting Up a System Access Printer

If the printer you want to use doesn't support desktop printing software, you can make the printer available as a system access printer. The system access printer becomes the default printer for the selected workgroup.

Users who can see the Chooser can select any printer visible to them. 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.

Note: You cannot use both regular desktop printers and a system access printer.

To set up a system access printer:

- 1 Create one or more computer lists containing client computers on which you plan to use system access printers.
- 2 For each workgroup you want to use a system access printer, make sure that workgroup has access to the computers in the list or lists you created.
- 3 Log in to a client computer using the System Access workgroup.
You see the System Access workgroup only if you are a Macintosh Manager administrator or if "User has System Access" is enabled for your account.
- 4 Select Chooser from the Apple menu.
- 5 Select and set up a printer, then choose Quit from the File menu and log out.
- 6 Repeat steps 3 through 5 for each client computer where users need access to a system access printer.
- 7 From the server or an administrator computer, open Macintosh Manager.
- 8 Click Workgroups, then click Printers.
- 9 Select a workgroup that has access to the computers you set up in the previous steps.
- 10 Select "Members use printer selected in System Access."
- 11 Click Save.

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.

Using Options Settings

Options settings are used to set up a group documents folder, create a login message for workgroups, set startup and login events, and allow users in Panels or Restricted Finder workgroups to eject CDs.

Choosing a Location for Storing Group Documents

You can use a group documents location to store folders and files you would like to make available to everyone in a workgroup. Once you have chosen a location and login settings for the group documents volume, you can set up shared folder access in the Privileges pane.

To set up a group documents volume:

- 1 In Macintosh Manager, click Workgroups, and then click Options.
- 2 Select a location for storing group documents in the “Stored on volume” pop-up menu.
- 3 If the volume doesn’t use the same user names and passwords used by Macintosh Manager, select “Prompt user for log-in.”

Users must enter a valid user name and password.

- 4 If you want to grant easy access to the group documents volume for all users, select “Log in automatically as this AFP user” and type in a valid user name and password.

This isn’t as secure as requiring users to log in with their own information, because you can’t control access individually or track who has logged in to the server.

- 5 If the group documents location is “Designated Macintosh Management Server,” you can choose “Log-in Automatically using the default name and password.”

The default name and password are internal to Macintosh Manager. You cannot track user login if you choose this setting.

You can select “Always try automatic log-in with user’s name and password first” in addition to the other settings. If this attempt at login fails, the login method you selected under “When mounting” is used.

- 6 Click Save.

If the location you want doesn’t appear in the menu, choose Other from the “Stored on volume” pop-up menu. You can only select volumes that are mounted on the server. If you still can’t find the volume you want, click Find and mount the appropriate volume.

Making Items Open at Startup

Give users a head start on their work by conveniently opening applications or folders for them when the computer starts up.

To open items at startup:

- 1 On each client computer, place the items you want to open at startup in the Startup Items folder in the Mac OS 9 or Mac OS 8 System Folder.
- 2 In Macintosh Manager, click Workgroups, and then click Options.
- 3 Select one or more workgroups in the Workgroups list.
- 4 Select “Open items in the Startup Items folder” and click Save.

For computers that start up using NetBoot, you must follow special procedures to copy items to the Startup Items folder on the startup disk image. See Chapter 12, “NetBoot,” for details.

Checking for Email When Users Log In

If a user has a Post Office Protocol (POP) email account, you can have Macintosh Manager check the mail server for messages when the user logs in.

To check for email automatically:

- 1 Open Macintosh Manager.
Before you proceed, click Computers, and then click Control. Check the incoming email server information and make sure it is correct. The incoming email server must be a POP server in order to check email at login.
- 2 Click Workgroups, then click Options.
- 3 Select “Check for email when members log in,” then click Save.

Creating Login Messages for Workgroups

You can display a message or announcement when a user logs in.

To create a workgroup login message:

- 1 In Macintosh Manager, click Workgroups, and then click Options.
- 2 Type a message in the Group Message box, then click Save.

Setting Up Computer Lists

You can use Macintosh Manager to manage computers by grouping several computers together and choosing settings for them. Once you create a list of computers you want to manage, you can select workgroups that are allowed to use them, and you can customize control settings, security settings, and login settings for each list. Checkout features are used to manage mobile computers such as iBooks.

This section tells you how to set up computer lists individually, by duplication, or by using a template.

Creating Computer Lists

Computer lists are simply groups of computers, in the same way that workgroups are groups of users. These lists appear under “Machine Lists” on the left side of the Computers pane. You can limit access to computers by assigning specific workgroups to the computers you want them to use. Computer lists are also useful if you want certain computers to have different settings.

A computer cannot belong to more than one list.

To set up a computer list:

- 1 In Macintosh Manager, click Computers, and then click Lists.
- 2 Click Add and give the new list a name.
The name can contain up to 31 characters (including period, underscore, dash, or space).
The name cannot contain a colon (:).
- 3 Click Find and choose or connect to a computer from the workstation selection window.
Repeat this step for each computer you want to appear in the list. To remove a computer from the list, select it and click Remove.
- 4 Make sure the login option is set to Enabled. Choose additional settings for the computer list in the other Computers panes, then click Save.

Setting Up the All Other Computers Account

Any settings selected for All Other Computers are applied to computers that connect to your managed network but do not appear in their own computer lists. These computers are also called guest computers.

To set up the All Other Computers account:

- 1 In Macintosh Manager, click Computers.
- 2 Select the All Other Computers account.
- 3 Choose the settings you want to use in each pane of the Computers pane, then click Save.

Duplicating a Computer List

You can easily create a computer list with the same settings as one you have already created. A duplicate list doesn't contain any computers because a computer cannot be in more than one list, but the settings are the same as the original.

To duplicate a computer list:

- 1 In Macintosh Manager, click Computers, and then click Lists.
- 2 Select an existing computer list and click Duplicate.
- 3 Type a new name for the list, then click Add to add computers to the list.
- 4 Click Save.

Creating a Computer List Template

You can use a template to apply the same initial settings to new computer lists. After you set up the template, each new computer list you add will have the template settings. You can change the computer list settings or the template settings at any time.

You cannot add computers to a template because computers cannot belong to more than one list.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To create a template for computer lists:

- 1 In Macintosh Manager, click Computers, and then select Template in the list of computer lists.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

- 2 In each Computers pane, set options you want to use for the template, then click Save.

Disabling Login for Computers

Occasionally, you may need to prevent user access on certain computers while you do maintenance tasks, such as installing and updating applications or running hard disk maintenance software. You can prevent access to computers by disabling login.

To prevent users from logging in on certain computers:

- 1 In Macintosh Manager, click Computers, and then click List.
- 2 Select a computer list, then set one of the login options explained in the steps that follow.
- 3 Select "Disabled--Ask User" to allow the user to choose to shut down the computer, go to the Finder (if the user has an administrator password), or pick a new Macintosh Manager server.
- 4 Select "Disabled--Go to Finder" to take the user to the Finder automatically.
- 5 Select "Disabled--Pick a different server" to allow the user to select another Macintosh Manager server from a list of local network servers.
- 6 Click Save.

To allow users to log in again, select Enabled in the login pop-up menu and click Save.

Using Workgroup Settings for Computers

You use settings in the Workgroups pane of the Computers pane to control access to computers.

Controlling Access to Computers

You can make computers available to everyone, or you can limit access to certain computers. If you want to allow specific workgroups to use only certain computers, make sure you have already set up the workgroups first. Then create a list of computers you want to make available to them, and follow the steps below.

The same workgroup can be added to more than one computer list.

To make computers available to workgroups:

- 1 In Macintosh Manager, click Computers, and then click Workgroups.
- 2 If you want to make computers available to everyone, select “All workgroups can use these computers.” To limit access to only certain workgroups, select “Allow only the following workgroups to use these computers.”
- 3 Select workgroups in the Available Workgroups list and click Add to add them to the Allowed Workgroups list. To remove an allowed workgroup, select it and click Remove.
- 4 Click Save.

If you want to disable access to certain computers, use one of the “disabled” login settings in the Lists pane of the Computers pane.

Using Control Settings

Control settings are used to set email settings in addition to options that affect the clock, hard disk name, and automatic disconnect.

Disconnecting Computers Automatically to Minimize Network Traffic

While a computer is connected to a network, even if no user is logged in, it looks for updates to databases on the server at regular intervals. On very large networks, you may notice delays in client response. You can ease the burden on your network by scheduling an automatic disconnect for computers when they are not in use.

To enable automatic disconnect:

- 1 In Macintosh Manager, click Computer, and then click Control.
- 2 Select a computer list, then select “Disconnect from the server if no user logs in within ___ minutes.”
- 3 Type in how many minutes the computer should wait before disconnecting.

- 4 Click Save.

When the computer disconnects from the server, the computer still displays the login screen, but an X appears over the server icon in the menu bar. Automatic updates will not occur again until a user logs in.

To reconnect a client, select a user and click Login. Then, click Cancel in the password dialog box.

Setting the Computer Clock Using the Server Clock

If your network doesn't have access to a Network Time Protocol server, you can synchronize the clocks on managed computers with the clock on the server.

To synchronize computer clocks:

- 1 In Macintosh Manager, click Computers, and then click Control.
- 2 Select a computer list, then select "Synchronize computer clocks with the server's clock."
- 3 Click Save.

Using a Specific Hard Disk Name

Specifying a certain name for a computer's hard disk can make it easier for some applications to locate information, such as preferences. Using a specific hard disk name is particularly useful if you use NetBoot. NetBoot clients have a startup volume named "NetBoot HD" by default. If the computers in a list use NetBoot, you should make sure the hard disk name is the same for NetBoot and non-Netboot computers. This ensures that the paths to all applications used on these clients are the same.

To use a specific hard disk name:

- 1 In Macintosh Manager, click Computers, and then click Control.
- 2 Select a computer list, then select "Force computer hard disk name to ___" and type in the name you want to use (for example, Macintosh HD).
- 3 Click Save.

Creating Email Addresses for Managed Users

Macintosh Manager can create an email address for a user who doesn't already have one. When a user logs in, Macintosh Manager adds the user's short name to the default domain name you specify and creates an email address.

If a user has other imported email settings, they will override Macintosh Manager's settings when the user connects to the Macintosh Manager network.

To create an email address for a user:

- 1 In Macintosh Manager, click Computers, and then click Control.

- 2 Select a computer list.
- 3 Under User Email Addresses, type the default domain name, the incoming (POP) mail server address, and the outgoing (SMTP) server address.
- 4 Click Save.

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.

Using Security Settings for Computers

Computer security settings let you choose security settings for users, computers, and applications.

Keeping Computers Secure If a User Forgets to Log Out

If a user doesn't log out when he or she finishes using a computer, other people can use the computer without logging in. They will have access to anything the previous user had access to, including that user's home directory and documents. You can prevent this type of unauthorized access with the idle logout feature.

Idle logout occurs when there is no user activity (such as typing or using the mouse) for a specified period of time. For example, suppose you enable idle logout after 15 minutes. A user logs in, works for a while, and then decides to leave the computer and go have a snack, but doesn't log out. After 15 minutes, the user returns and must enter a user name and password again to gain access.

To enable idle logout:

- 1 In Macintosh Manager, click Computers, and then click Control.
- 2 Select a computer list, then select “Enable idle log-out” and enter the number of minutes the computer should wait.
- 3 Choose a logout option.

If you select “Log user out,” users see a dialog box after idle log out and have the opportunity to save any unsaved documents, and then they return to the login screen.

If you select “Lock the screen,” the screen goes black and a dialog box appears. Users can save any unsaved documents, and then they can either enter a password and continue working or log out.

- 4 Click Save.

If this feature has been activated and the computer is connected to the network, you can use a Mac OS X Server administrator password to log in.

Allowing Access to All CDs and DVDs

Using computer security settings, you can allow user access to CDs and DVDs with no restrictions.

To allow access to any CD or DVD:

- 1 In Macintosh Manager, click Computers.
- 2 Click Security and select a computer list.
- 3 Select “Access all CD-ROMs” and click Save.
- 4 Select “Show a panel for inserted CD-ROMs” to make it easy for Panels workgroups to find inserted CDs.

Allowing Access to Specific CDs or DVDs

You can restrict user access to CDs and DVDs by using a list of approved discs. You can also allow users to access only certain files on a CD or DVD.

First, create the list of approved discs and items, and then allow user access to the discs.

To allow access to only specific CDs or DVDs:

- 1 In Macintosh Manager, make sure you have already set up a list of approved discs and items in the CD-ROMs pane of the Global pane.
See “Using Global CD-ROM Settings” on page 465 for instructions.
- 2 Click Computers, then click Security and select a computer list.
- 3 Select “Access approved CD-ROMs only.”
- 4 Select “Show a panel for inserted CD-ROMs” to make it easy for Panels workgroups to find inserted CDs.

Choosing Computer Security Settings for Applications

Some applications may occasionally use “helper applications” to do jobs they cannot do themselves. For example, if a user clicks a Web link in an email message, the email application might want to open a Web browser. Other applications, such as installers, may need to quit the Finder and restart in order to finish their jobs.

Important Macintosh Manager does not automatically allow these options, but you may choose to do so. Allowing these options can weaken computer security.

To allow applications to open other applications or quit the Finder:

- 1 In Macintosh Manager, click Computers, and then click Security and select a computer list.
- 2 Select “Open other applications, such as helper applications” and/or select “Quit the Finder” to allow these options for applications.

- 3 Click Save.

Allowing Specific Applications to Be Opened by Other Applications

You can allow specific applications to act as helper applications for other applications that might need to use them. The applications you want to designate as helpers must already be added to the list of allowed items for one or more workgroups.

To specify helper applications:

- 1 Open Macintosh Manager.
- 2 Choose Application Preferences from the Configure menu.
- 3 Select an application from the list.

The list only shows applications currently assigned to workgroups. If the application you want isn't in the list, click Add to browse for the application, or click Custom and type in the name and four-character code of the application you want to add.

- 4 To designate the application as a valid helper, select "Allow this application to be opened by other applications."

Allowing Users to Work Offline

If the Macintosh Manager server or a user's home directory is not available, you can still allow offline computer use. The user must log in, but the Macintosh Manager server is not available. If the home directory is not available, users may not be able to save their documents.

To allow users to work offline:

- 1 In Macintosh Manager, click Computers.
- 2 Click Security and select a computer list.
- 3 Select "Work offline if the Macintosh Manager Server is not available" to allow this option for users. If you want, you can also select "Require an Administrator password to work offline" for this option.
- 4 Select "Work offline if the user's home directory is not available" to allow this option for users.
- 5 Click Save.

Allowing Users to Switch Servers After Logging In

Ordinarily, after users log in, they cannot switch to another managed server without an administrator password. However, you can allow users this privilege.

Important Allowing this option can decrease server security. Also, if you have servers that use older versions of Macintosh Manager, switching a client computer to one of these servers may cause the server to install the older software on the client computer.

To allow users to switch servers:

- 1 In Macintosh Manager, click Computers.
- 2 Click Security and select a computer list.
- 3 Select “Switch to another server without authentication” to allow this option for users.
- 4 Click Save.

If you want NetBoot client computers to choose a different Macintosh Manager server, remove the DNSPlugin extension from the NetBoot image.

Allowing Users to Force-Quit Applications

If you allow users to force-quit applications, they can press Command-Option-Esc to force an application to quit.

Note: Allowing this option may pose a security risk.

To allow users to force-quit:

- 1 In Macintosh Manager, click Computers.
- 2 Click Security and select a computer list.
- 3 Select “Force Quit applications” to allow this option for users.
- 4 Click Save.

Allowing Users to Disable Extensions

If users are allowed to restart computers, you can also allow them to turn off extensions by pressing the Shift key during startup. This will not disable the Macintosh Manager extension or necessary system extensions.

Note: Allowing this option may pose a security risk.

To allow users to start up with extensions off:

- 1 In Macintosh Manager, click Computers.
- 2 Click Security and select a computer list.
- 3 Select “Disable extensions during startup” to allow this option for users.

- 4 Click Save.

Using Computer Login Settings

Computer login settings allow you to choose how users log in, what messages they see, and what panel names look like.

Choosing How Users Log In

When users log in to a computer, they can either type their names or choose their names from a list. If you decide to use a list for login, the list can contain up to 2000 users. You can choose not to display administrators in that list.

To set login options:

- 1 In Macintosh Manager, click Computers.
- 2 Click Log-In and select a computer list.
- 3 Select “Users choose their name from a list (1-2000 users)” to use the list option. If you do not want administrator names to appear in the list, select “List displays users only (no administrators).”
- 4 If you do not want to use a list, select “Users type their name.”
- 5 Click Save.

Creating Login Messages for Computers

You can create two types of messages for computers. Each can contain up to 127 characters.

- The banner message appears in the login dialog box.
- The server message appears in a separate panel after users log in. It is preceded by the phrase “From: Global Administrator.”

To set up a login message:

- 1 In Macintosh Manager, click Computers.
- 2 Click Log-In and select a computer list.
- 3 Type your banner message or server message in the appropriate message text box.
If you do not want to use a message, leave the text box blank.
- 4 Click Save.

Customizing Panel Names

You can customize the names of the workgroup and user documents panels shown for Panels workgroups.

To customize a panel name:

- 1 In Macintosh Manager, click Computers.
- 2 Click Log-In and select a computer list.
- 3 If you want the workgroup's name to appear on a workgroup documents panel, select "Show the workgroups name" or click the button next to the text box and type a different name.
- 4 If you want the user's name to appear on a user document panel, select "Show the user's name" or click the button next to the text box and type a different name.
- 5 Click Save.

Managing Portable Computers

It is important to plan how you want to manage portable computers that have access to your network. This section gives suggestions for managing portable computers and tells you how to use Macintosh Manager's checkout feature.

Portable Computers With Network Users

You can let users share specific portable computers, such as those in an iBook Wireless Mobile Lab. An iBook Wireless Mobile Lab contains either 10 or 15 student iBooks (plus an additional iBook for an instructor), an Airport base station, and a printer, all on a mobile cart. The cart lets you take the computers to your users (for example, from one classroom to another).

To manage the mobile lab, first create a computer list containing all of the iBooks. Make sure users have network accounts and home directories, and then assign sets of users to workgroups that will use the iBooks. You might want to create different workgroups for different purposes, such as one for a history class, one for a biology class, and so on. You can use the Check Out feature to allow these workgroups to use the iBooks.

You can use the All Other Computers account to manage network users who have their own portable computers. See "Providing Quick Access to Unimported Users" on page 429 for more information.

Portable Computers With Local Users

Local user accounts cannot be managed using Macintosh Manager. However, you can use the Multiple Users control panel to set up local user accounts on specific computers in one of two ways:

- The user does not have administrator privileges, but has a local account.
- The user is the administrator for the computer.

If the user is the local administrator, he or she has total access to the all folders and applications on the computer, including the System Folder.

Letting Users Check Out Computers

You can allow users to check out and take home a portable computer (to continue working on a project after school, for example). Macintosh Manager settings and security features remain in effect on the computer even while it is checked out.

To check out a computer:

- 1 In Macintosh Manager, click Computers.
- 2 Click Check Out and select a computer list.
- 3 Select “These computers can be Checked Out” and then select one of the checkout options in the steps that follow.
- 4 Select “All users are allowed to Check Out these computers” to allow this option.
- 5 Select “Allow only the following users to Check Out these computers” to restrict checkout to a list of specific users. Then, select users in the Available Users list and click Add to make them allowed users.

To remove users from the Allowed user list, select one or more users and click Remove.

- 6 Click Save.

Using Wireless Services

You can provide wireless network service to managed clients using AirPort, for example. Make sure the Macintosh Manager Server is within range of your wireless service. If a user on a portable computer goes out of range, he or she cannot log in to Macintosh Manager, but you can allow the user to work offline. See “Allowing Users to Work Offline” on page 458 for more information.

If you need more information about using AirPort, consult AirPort documentation or visit the Web site:

www.apple.com/airport/

Using Global Security Settings

In Macintosh Manager, global security settings apply to your entire Macintosh Manager network (all users, groups, and computers). These settings cover a variety of options that affect reports, guest access, passwords, and how preferences are copied.

Using Macintosh Manager Reports

Macintosh Manager provides a number of different reports to help you keep track of user and network activity.

To view a report:

- 1 Open Macintosh Manager.
- 2 Choose the report you want from the Reports menu.

You can view the selected report immediately, and then export it to a file or print it if you wish.

You can set additional criteria for the Activity Log report and the Computers report before you see the results.

Setting the Number of Items in a Report

You can set the maximum number of log entries to show for Macintosh Manager reports.

Note: The Connected Users report will show only up to 300 log entries, even if the maximum number of log entries you set is greater than 300.

To set how many log entries are tracked:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 In the text box next to “Maximum number of log entries,” type a number.

To view a report, go to the Report menu and choose the report you want to see.

Keeping the Administration Program Secure

If an administrator forgets to quit the Macintosh Manager administration application, another person could potentially make changes and save them. To prevent this kind of unauthorized access, you can make the administration application quit after a specified time if there is no user activity.

Warning When the administration application quits automatically, unsaved changes are lost.

To allow the administration program to quit automatically:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 Select “Quit the administration program if idle for ___ minutes” and enter the number of minutes the application should wait before quitting automatically.
- 3 Click Save.

Verifying Login Information Using Kerberos

If all users must authenticate using Kerberos, follow the steps below. For more information about using Kerberos, see “Using Kerberos” on page 197.

To use Kerberos verification:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 Select “Clients must authenticate using Kerberos” and click Save.

Preventing Users From Changing Their Passwords

Ordinarily, all users can change the passwords assigned to them. If you don’t want users to change their own passwords, you can remove that privilege.

To keep users from changing their passwords:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 If “Users can change their passwords” is selected, deselect it.
- 3 Click Save.

Allowing Administrators to Access User Accounts

You can allow a system administrator to log in as any user. The user can enter the user name for the account he or she wants to access and use the appropriate administrator password.

To allow administrators to log in as other users:

- 1 In Macintosh Manager, click Global, and then click Security.
- 2 Select “Users may log in using a server administrator’s password.”
- 3 Click Save.

Copying Preferences for Mac OS 8 Computers

Users on Mac OS 8 computers can make changes to preferences while they are logged in (for example, they can change the desktop picture). However, when users log out, their preferences are saved only if you allow them to be saved. Macintosh Manager provides two ways to control how preferences are copied for Mac OS 8 users.

- If you want to save all preference changes for each user, you can copy the entire Preferences folder. Macintosh Manager will copy every item in the folder, regardless of what it is or how big it is. Copying unnecessary or large items can increase login and logout times for Mac OS 8 clients. For more information, see “Preserved Preferences” on page 468.

- If you want to limit the preferences copied, you can choose to copy only Internet preferences and administrator-defined preferences. Preference folders for Web browsers are copied, but the cache folders inside them are deleted. Using this option can significantly lighten the load on the server and have less of an impact on login and logout times.

If you use this option, Macintosh Manager will always copy the following preference files and folders:

Explorer (cache folder inside is deleted)

Fetch Preferences

Internet Preferences

JPEGView Preferences

NCSA Telnet Preferences

Netscape *f* (cache folder inside is deleted)

Newswatcher Preferences

RealAudio Player Preferences

StuffIt Expander Preferences

To set how Mac OS 8 user preferences are copied:

1 In Macintosh Manager, click Global, and then click Security.

2 Select one of these options:

To copy all preference items, select “Copy entire Preferences folder.”

To copy only certain preference items, select “Copy only Internet or administrator-defined preferences.”

3 Click Save.

Using Global CD-ROM Settings

Global CD-ROM settings let you allow access to all CDs and DVDs or to only a specific list of discs. When you make a disc available to Macintosh Manager, you can view its contents, and then you can allow users access to all items on the disk or just the items you select.

Note: These settings do not apply to audio CDs. The audio CD setting is in the Privileges pane of the Workgroups pane.

To create a list of available discs and disc items:

1 In Macintosh Manager, click Global, and then click CD-ROMs.

2 Insert a CD or DVD.

- 3 Select the disc name and click Add to make it available in Macintosh Manager. To remove an available item, select it and click Remove.
- 4 To make specific items on a disc available to users, select a CD or DVD in the “Available in Macintosh Manager” list.

In the “Allowed items on ()” list, select items you want to make available to users. Click Allow All to select and allow every item on the disc. Click Allow None to deselect all items.

- 5 When you have finished, click Save.

To make only your list of approved items available to users, select a computer list and make sure to select “Access approved CD-ROMs only” in the Security pane for Computers. You may also want to select “Show a panel for inserted CD-ROMs” to make it easy for Panels workgroups to find inserted CDs.

Managing Preferences

You can use the Managed Preferences folder to customize how application preferences and system preferences are handled to meet your particular needs and goals. For example, you can make sure that users always start out with a specific set of preferences or that some user-set preferences are never overridden.

A Managed Preferences folder is created on the workgroup data volume the first time any member of a workgroup logs in. Inside this folder are either two or three (initially empty) additional preference folders, depending on the client operating system:

Client operating system	Contents of Managed Preferences folder
Mac OS 9	Initial Preferences folder Forced Preferences folder
Mac OS 8	Initial Preferences folder Forced Preferences folder Preserved Preferences folder

Using Initial Preferences

Preferences in the Initial Preferences folder are set once during login. The first time users log in, they get a fresh copy of any preferences contained in the Initial Preferences folder. Users can modify these preferences, and the changes are saved at logout.

For example, in a classroom setting, a teacher can set up preferences and a list of bookmarks for a particular Web browser. He or she stores a copy of those preferences in the Initial Preferences folder. When students log in on the first day of class, they all start out with the same browser preferences and the same list of bookmarks.

After a user's first login, Macintosh Manager checks the user's Preferences folder and compares it to the contents of the Initial Preferences folder. If a user already has a preference in the folder, Macintosh Manager doesn't replace that preference. If a user's folder doesn't contain one or more initial preferences, Macintosh Manager copies the missing files to the user's folder.

This process is repeated each time a user logs in, so you can place additional preference files in the Initial Preferences folder later. For example, if you install new software and place the software preferences file in the Initial Preferences folder, Macintosh Manager copies the new file to a user's Preferences folder when the user opens the new software for the first time.

To use the Initial Preferences folder:

- 1** Set up a workgroup data volume (Group Documents) in the Options pane of the Workgroups pane.
- 2** From a client computer, access the group documents volume.
- 3** Create any preferences you want to place in the Initial Preferences folder.
- 4** Copy the preferences you created to the Initial Preferences folder on the group documents volume.
- 5** Repeat steps 1 through 4 for each group documents volume.

Exceptions to Initial Preferences

A few preferences are created automatically the first time a user logs in, regardless of whether you're using an Initial Preferences folder. You don't need these items in the Initial Preferences folder because they won't be copied to the user's folder:

- Apple Menu Options Preferences
- AppSwitcher Preferences
- Internet Preferences
- Keyboard Preferences
- Keychains
- Location Manager Preferences
- Mac OS Preferences
- TSM Preferences
- User Preferences

Using Forced Preferences

Using the Forced Preferences folder lets you ensure that users start out with a specified set of preferences every time they log in. If a user changes his or her preferences, those preferences are replaced with the preferences in the Forced Preferences folder the next time the user logs in.

Forced preferences are copied to the appropriate location depending upon the client operating system. The processes are explained below.

- *Mac OS 9 clients:* When a user logs in, Macintosh Manager compares preference folders and files in the /Library/Classic folder of a user's home directory to items in the Forced Preferences folder. Macintosh Manager deletes any matching items from the user's folder and replaces them with preferences from the Forced Preferences folder. If any forced preferences are missing from the user's folder, Macintosh Manager places new copies of these items in the user's Preferences folder.

If there are items in the user's Preferences folder that do not match any items in the Forced Preferences folder, Macintosh Manager does nothing to them. If you have concerns about these items accumulating or consuming disk space, clean out the user's Preferences folder occasionally.

- *Mac OS 8 clients:* When a user logs in, Macintosh Manager copies items 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.

To use forced preferences:

- 1 Set up a workgroup data volume (Group Documents) in the Options pane of the Workgroups pane.
- 2 From a client computer, access the group documents volume.
- 3 Create any preferences you want to place in the Forced Preferences folder.
- 4 Copy the preferences you created to the Forced Preferences folder on the group documents volume.
- 5 Repeat steps 1 through 4 for each group documents volume.

Preserved Preferences

The Preserved Preferences folder is available only for Mac OS 8 client computers. The files and folders that you put in the Preserved Preferences folder are never actually copied. Instead, Macintosh Manager creates a list containing the names of all the folders and files inside the Preserved Preferences folder. Macintosh Manager uses this list to determine which preferences need to be copied between the server and the client computer during login and logout. Because you can limit which preferences are copied, using the Preserved Preferences folder can help you decrease login and logout time for Mac OS 8 clients.

When you use Preserved Preferences, this is what happens during login and logout on a Mac OS 8 client:

- *When a user logs in:* Macintosh Manager scans the Preserved Preferences folder and builds a list containing the names of the files and folders inside. Macintosh Manager automatically adds the names of the preferences that are always copied to create a combined list. Next, Macintosh Manager copies all the files and folders on 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 and replaced. 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.

To use preserved preferences:

- 1 Set up a workgroup data volume (Group Documents) in the Options pane of the Workgroups pane.
- 2 From a client computer, access the group documents volume.
- 3 Create any preferences you want to preserve for users.
- 4 Copy the preferences you created to the Preserved Preferences folder on the group documents volume.

Alternatively, you can set up Preserved Preferences using “placeholders” instead of the actual preferences, as long as the name and type of the placeholder match the name and type of the preference. For example, if an application's preferences are in a folder called “MyApp Prefs,” you can create an empty folder named “MyApp Prefs” in the Preserved Preferences folder.

- 5 Repeat steps 1 through 4 for each group documents volume.

The table below lists certain preferences that are always copied, and other preferences that are never copied. You do not have to include any of these preferences in the Preserved Preference folder.

Always copied	Never copied
Control Strip Preferences	AppleTalk Preferences
Date & Time Preferences	Client Preferences
Finder Preferences	ColorSync Profiles

Always copied	Never copied
Mac OS Preferences	Desktop Picture Preferences
Panels Preferences	Energy Saver Preferences
	Extensions Manager Preferences
	Multi-User Items
	Multi-User Preferences
	Open Transport Preferences
	Remote Access
	TCP/IP Preferences
	Users & Groups Data File
	Users & Groups Data File Backup

Solving Problems

This section describes some problems you may encounter while using Macintosh Manager and provides troubleshooting tips and possible solutions. If your problem is not addressed here, you may want to check Macintosh Manager Help or consult the AppleCare Knowledge Base online.

I've Forgotten My Administrator Password

Contact your Mac OS X Server administrator if you forget your password. If necessary, the server administrator can change your password using the Workgroup Manager application.

Administrators Can't Get to the Finder After Logging In

If you have system access, you can choose the System Access workgroup when you log in. If you don't have system access, and you need to go to the Finder often, ask your Macintosh Manager administrator to enable system access for your account.

You can bypass Macintosh Manager login by pressing Command-Shift-Esc when the Welcome dialog box appears. Then enter either the computer owner's password or a local administrator's name and password.

Generic Icons Appear in the Items Pane

If generic icons appear in the Items pane of the Workgroups pane in Macintosh Manager, restart the computer with Mac OS 9 and rebuild the Desktop file.

Selecting “Local User” in the Multiple Users Control Panel Doesn’t Work

You cannot use both Macintosh Manager client software and the Multiple Users control panel on the same computer.

If you want to set up local users, do not install Macintosh Manager client software on the computer. Instead, install the Multi-User Startup extension and use the Multiple Users control panel version 1.4.1.

Some Printers Don’t Appear in the Available Printers List

When you make printers available to client computers, Macintosh Manager creates desktop printers for your Mac OS 9 clients. The Mac OS X version of the Macintosh Manager administrator application creates only LaserWriter desktop printers. If you need to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients.

Users Can’t Log In to the Macintosh Manager Server

First, make sure the server has enough free disk space. If the user’s password has not been changed and his or her user account has not been deleted, check the user’s Macintosh Manager login privileges.

To make sure login is enabled:

- 1 In Macintosh Manager, click Users, and then click Basic.
- 2 Make sure “User can log in” is selected. If “Disable login as of ___” is also selected, make sure the date has not already passed.

Users Can’t Log In as “Guest” on Japanese-Language Computers

If users need to log in using the Guest account on Japanese-language client computers, you must change the computer’s language script to Roman in the International pane of System Preferences.

A Client Computer Can’t Connect to the Server

Try doing the following:

- Make sure the server is running. If you recently started the server, it may take a few minutes for the server to appear.
- Make sure network information (including DNS information) is entered correctly.
- Make sure the client computer is not low on memory and that it is connected to the network.
- If many computers start up at once, the load on your network may be too great. Try starting fewer computers at one time.

The Server Doesn't Appear in the AppleTalk List

Mac OS X Server does not support AppleTalk network connections to Apple Filing Protocol (AFP) servers, such as the Macintosh Manager server. To connect to AFP servers, set client computers to connect via TCP/IP.

Macintosh Manager client computers can, however, use AppleTalk for service discovery. If your network has AppleTalk zones, users on Mac OS 8 computers may need to select the zone where the server resides. On Mac OS 9 computers, use the Network Browser to make sure you are connected to the server.

The User's Computer Freezes

If the computer's system software is earlier than Mac OS 9, make sure file sharing is turned off.

Users Can't Access Their Home Directories

Users may see a message if their home directories cannot be found at login.

In Workgroup Manager, make sure the user's home directory exists and has the correct permissions settings. Then, make sure the server that contains the user's home directory is connected.

Users Can't Access Shared Files

Shared workgroup folders are normally located on the same server volume. However, if you store workgroup documents on more than one volume, some users may not be able to access all of their shared documents without changing workgroups.

If the user belongs to more than one workgroup and workgroup documents are stored on several servers, make sure the user has the latest version of AppleShare.

Shared Workgroup Documents Don't Appear in a Panels Environment

If you created a workgroup data volume but users in a Panels workgroup can't see it, make sure the workgroup data volume contains the shared documents folders.

Also check to make sure the location of the Users folder has not changed. The Users folder is usually located at the top level of either the server volume or the workgroup data volume.

Applications Don't Work Properly or Don't Open

Some applications write to or create special files in places other than the Preferences folder inside the System Folder. If you enforce file-level security for a workgroup, some older applications may not function properly or may report errors. See "Preventing Applications From Altering Files" on page 441 for more information.

You can create a folder called “Other Applications •” and then put the Applications folder (and all of its contents) inside. The Other Applications • folder must reside in the client computer’s Applications folder. If the client computer is running Mac OS 9.1 or later, the Applications folder is called “Applications (Mac OS 9).”

Users Can’t Drag and Drop Between Applications

In most cases, Macintosh Manager does not allow the drag-and-drop feature. Use the Copy and Paste commands instead.

Users Can’t Open Files From a Web Page

Sometimes Web browsers rely on helper applications to open files that the browser itself cannot handle (for example, media files or PDF files).

- 1** In Macintosh Manager, click Computers, and then click Security.
- 2** Select “Open applications, such as helper applications.”

Sometimes the Right Application Doesn’t Open for Users

If the wrong application opens when a user tries to open a document, try rebuilding the client computer’s desktop.

Where to Find More Information

The AppleCare Web site provides a variety of resources, including the Knowledge Base (a database containing technical articles about product usage, implementation, and problem solving). Investigate the Web site at

www.apple.com/support

Discussion lists for 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

www.lists.apple.com

DHCP Service

Dynamic Host Configuration Protocol (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 on your network. If a DHCP server is found, the client computer then requests an IP address. 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 Settings to

- configure and administer DHCP service
- create and administer subnets
- configure DNS and NetInfo options for client computers
- view DHCP and NetBoot client computers

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 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 for 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. Each subnet needs a way to connect to the other subnets. A hardware device called a router typically connects subnets.

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 short leases, DHCP can reassign IP addresses on networks that have more computers than 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 Web servers. Other devices that need to be continuously available to network users, such as printers, may also benefit from static IP addresses.

Static IP addresses can be set up either by manually entering the IP address on the computer or device or by configuring DHCP to provide the same address to a specific computer or device on each request. DHCP-assigned addresses allow configuration changes at the DHCP server. Manually configured static IP addresses avoid possible issues certain services may have with DHCP-assigned addresses and avoid the delay required for DHCP to process the request.

Server Settings does not provide a way to assign static IP addresses using the BootP protocol (the protocol underlying DHCP). To assign static IP addresses, you can use the NetInfo Manager application in Mac OS X to create the appropriate properties in the local NetInfo database. See “Configuring Static Ports for Shared NetInfo Domains” on page 113 for more information on setting up static IP addresses on local networks.

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 or a router on your network that can relay BootP communications, it will work for DHCP. If you don't have a relay, you need to place the DHCP server on the same subnet as your clients.

Interacting With Other DHCP Servers

You may already have other DHCP servers on your network, such as AirPort base stations. Mac OS X Server can coexist with other DHCP servers as long as each DHCP server uses a unique pool of IP addresses. However, you may wish your DHCP server to provide an LDAP server address for client auto-configuration in managed environments. AirPort base stations cannot provide an LDAP server address. Therefore, if you wish to use the auto-configuration feature you must set up AirPort base stations in Ethernet bridging mode and have Mac OS X Server provide DHCP service. If the AirPort base stations are on separate subnets, then your routers must be configured to forward client broadcasts and DHCP server responses as described previously. If you wish to provide DHCP service with AirPort base stations then you cannot use the client auto-configuration feature and you must manually enter LDAP server addresses at client workstations.

Assigning Reserved IP Addresses

Certain IP addresses can't be assigned to individual hosts. These include addresses reserved for loopback and addresses reserved for broadcasting. 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 you 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 settings for each step in “Managing DHCP Service” on page 478.

Step 1: Create subnets

The following instructions show you how to create a pool of IP addresses that are shared by the client computers on your network. You create one range of shared addresses per subnet. These addresses are assigned by the DHCP server when a client issues a request.

To create subnets:

- 1 In Server Settings, click the Network tab, 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.)
- 2 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. You may need to set the DNS server address. See “Setting the Default DNS Server for DHCP Clients” on page 479 for more information.

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. For more information on setting up logs for DHCP service, see “Setting Up Logs for DHCP Service” on page 480.

Step 3: Start DHCP Service

Start DHCP service from Server Settings.

To start DHCP service:

- 1 Click DHCP/NetBoot.
- 2 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.

Managing DHCP Service

This section describes how to set up and manage DHCP service on Mac OS X Server.

Starting and Stopping DHCP Service

Follow these steps when starting or stopping DHCP.

To start or stop DHCP service:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Start DHCP or Stop DHCP.

As the service is starting up or shutting down, a globe flashes on the DHCP/NetBoot icon. When the service is turned on, the globe appears on the DHCP/NetBoot icon. It may take a moment for the service to start (or stop).

Setting the Default DNS Server for DHCP Clients

The first time you connect to a Mac OS X Server using Server Settings, the DHCP client module does not use the DNS server IP address you entered in the Setup Assistant. You must set the default address in the DHCP module of Server Settings.

To configure DHCP to use the correct DNS server:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Click the DNS tab.
- 5 Click Use Defaults, then click Save.

Setting the LDAP Server for DHCP Clients

You can use DHCP to provide your clients with LDAP server information rather than manually configuring each client's LDAP information.

To configure DHCP to provide the LDAP server address:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Click the LDAP tab.
- 5 Enter an LDAP server name and search base.
- 6 Enter a port or leave the field blank to use the default port.
- 7 Select "LDAP over SSL" if you wish LDAP information to be encrypted with SSL.

SSL must be enabled on your server to use this option.

- 8 Click Apply to add the server to the LDAP Servers list at the top of the pane.

The order in which the LDAP servers appear in the list determines their search order in the automatic Open Directory search policy.

- 9 Click New to clear the entry fields and enter additional LDAP server information.

If you wish to delete a server from the list, click the server name and then click Delete.

To modify a listed server, click the server name. Edit the name, search base, port, and SSL settings. Click Apply to update the LDAP Servers list.

- 10 Click Save when finished to save changes to the LDAP Servers list.

Setting Up Logs for DHCP Service

You can choose the level of detail you want to log for DHCP service.

- “Log warnings and errors only (normal)” can alert you to conditions in which data is inconsistent, but the DHCP server is still able to operate.
- “Log serious errors only (quiet)” will indicate conditions for which you need to take immediate action (for example, if the DHCP server can’t start up).

To set up logs for your DHCP server:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Click the Logging tab and select the logging option you want.

Deleting Subnets From DHCP Service

You can delete subnets and subnet IP address ranges.

To delete subnets or address ranges:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet or a subnet address range and click Delete.

Changing Lease Times for Subnet Address Ranges

You can change how long IP addresses in a subnet are available to client computers.

To change the lease time for a subnet address range:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Enter a number in the Lease Time field and choose a value from the pop-up menu.
- 5 Click Save.

Click Use Defaults 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.

Monitoring DHCP Client Computers

The DHCP client list shows the following information for each client computer in the database:

- DHCP client ID
- computer name
- hardware address
- IP address served to the client
- lease time left

To view the DHCP client list:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose View DHCP Clients.
- 3 Click Refresh to update the list.

Click any column heading to sort the list by different criteria.

Creating Subnets in DHCP Service

Subnets are groupings of client computers on the same network that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). Each subnet has at least one range of IP addresses assigned to it.

To create a new subnet:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Click New, or select an existing subnet and click Duplicate.
- 4 Enter the name of the new subnet and choose a port from the pop-up menu.
- 5 Enter a beginning and ending IP address for this subnet range.
Addresses must be contiguous, and they can't overlap.
- 6 Enter the subnet mask and router for this subnet, then click Save.

Click Use Defaults 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.

To use the Mac OS X Server for the gateway for the subnet, enter the server IP address in the router field.

Changing Subnet Settings in DHCP Service

Use Server Settings to make changes to DHCP subnet settings.

To change subnet settings:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Make the changes you want.
- 5 Click Save.

You can click Use Defaults to use the server's default settings.

Setting DNS Options for a Subnet

You can decide which DNS servers and default domain name a subnet should use. DHCP service provides this information to the client computers in the subnet.

To set DNS options for a subnet:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Click the DNS tab.
- 5 Enter the IP addresses of the DNS servers you want this subnet to use.
- 6 Enter the default domain name associated with the subnet, then click Save.

If you click Use Defaults, DHCP service gets DNS information from a DNS lookup that supplies the domain name and default DNS servers.

Setting NetInfo Options for a Subnet

You can give client computers in a subnet access to the information in NetInfo databases by “binding” the clients to one or more NetInfo parent servers.

You need to know the file name of the NetInfo database (or NetInfo tag) you want to use and the IP address of the server that hosts that database (or domain). The NetInfo tag is “network” if the domain was created using NetInfo Domain Setup.

To set NetInfo options for a subnet:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet and click Edit.
- 4 Click the NetInfo tab.
- 5 Enter the NetInfo tag of the NetInfo domain for this subnet.

- 6 Enter the IP address of each NetInfo parent server, then click Save.
Click Use Defaults if you want to use the server's default NetInfo settings.

Disabling Subnets Temporarily

You can temporarily shut down a subnet without losing all its settings.

To disable a subnet:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP.
- 3 Select a subnet address range and click Edit.
- 4 Deselect Enable DHCP in the General pane, then click Save.

Viewing DHCP and NetBoot Client Lists

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 client list shows the following information for each connected client computer:

- path to the startup disk image used by the client
- clients' Ethernet address (from the TCP/IP control panel)
- system software version and type of computer

To view the DHCP or NetBoot client list:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose View DHCP Clients or View NetBoot Clients.
- 3 Click Refresh to update the list.

Click any column heading to sort the list by different criteria.

Viewing DHCP Log Entries

If you've enabled logging for DHCP service, you can check the system log for DHCP errors.

To see DHCP log entries:

- 1 In Server Settings, click the General tab.
- 2 Click Log Viewer and choose System Software.
- 3 Choose System Log from the pop-up menu and look for entries that begin with “bootpd.”

Solving Problems

- Examine logs to pinpoint problems.
- Try a different client to determine whether the problem is with the client or the server.

Where to Find More Information

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 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 DHCP, see:

- *DCHP*: RFC 2131

NetBoot

NetBoot lets you start up Macintosh client computers from disk images on a Mac OS X Server. A *disk image* is a file that looks and acts like a mountable disk or volume. NetBoot disk images that contain system software can be used as a startup disk by client computers on the network.

By creating Mac OS disk images on a server, you can have your Macintosh client computers start up from a standardized Mac OS configuration. You can ensure that all the clients are running the same system software, which is properly configured for the tasks users will be doing on their computers. Because the client computers are all starting up from the same disk image, you can quickly update the operating system for the entire group by changing the configuration of the disk image from which they start. You can also use NetBoot to start up other Mac OS X Servers.

Mac OS X Server allows you to create set up than one disk image. This lets you provide custom Mac OS environments for different groups of clients. You can also create disk images containing application software.

You use the following Mac OS X Server applications to set up and administer NetBoot:

- *Network Image Utility*—to create Mac OS X disk images. The Network Image Utility is installed with Mac OS X Server software, in the Utilities folder.
- *NetBoot Desktop Admin*—to modify the Mac OS 9 system disk image and accompanying disk image for applications.
- *Server Settings (DHCP/NetBoot pane of the Network tab)*—to enable and configure NetBoot on the server.
- *PropertyListEditor*—to edit property list (plist) files (used primarily when creating custom packages for Network Install images)
- *Package Maker*—to create package files that can be included on disk images.

You can use Mac OS X client management services to provide a personalized work environment for any NetBoot client computer user. For information about client management services, see Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8.”

The Mac OS X Server product includes the following CDs that contain applications and files specific to NetBoot:

- *Mac OS X Server Administration Tools* CD
 - NetBoot, Network Install *f*—includes Network Image Utility (in Image Creation *f*) and Package Maker and PropertyListEditor (in Image Manipulation *f*)
 - *NetBoot, Mac OS 9* CD
 - About NetBoot.pdf (Read Me file)
 - NetBoot Desktop Admin *f*—contains About NetBoot Desktop Admin (Read Me file) and NetBoot Desktop Admin
 - NetBoot.pkg—contains the preconfigured Mac OS 9.2.2 system disk image
- Note:** The contents listed above are localized into four languages: English, French, German, and Japanese. Each localized set appears in a separate folder on the CD labeled by language.

Prerequisites

Warning Setting up your server to use NetBoot requires that you have the authority (authorization privileges) as well as the expertise to make changes to your network configuration. Potential risks include loss of data, client computers that can't start up, and failure of the network.

Administrator Requirements

If you want to set up NetBoot on your server, you should meet the following requirements:

- You are the server administrator.
- You are familiar with Network Setup.
- You know the DHCP configuration.

You will also need to work with your networking staff who can configure network topologies, switches, routers, and other network settings.

Server Requirements

Your server must meet the following requirements:

- DHCP service (either provided by this server or elsewhere on your network)
- Ethernet:
 - 100 Mb (for fewer than 10 clients)
 - 100 Mb switched (for 10–50 clients)
 - Gigabit (more than 50 clients)

These are estimates for the number of clients supported. See “Capacity Planning” on page 488 for a more detailed discussion of the optimal system and network configurations to support the number of clients you have.

NetBoot is not supported over wireless connections.

Client Computer Requirements

Any Macintosh computer that can run Mac OS 9.2.2 (all Macintosh computers released since the iMac) can use Netboot to start up from a Mac OS X Server disk image. At the time of this publication, this includes the following Macintosh computers:

- iMac
- iBook
- eMac
- Power Macintosh G3 (blue and white)
- Power Mac G4
- Power Mac G4 Cube
- PowerBook (FireWire)
- PowerBook G4
- Xserve

Note: You should install the latest firmware updates on all client computers. Firmware updates are available from the Apple support Web site:

www.apple.com/support/

Older Macintosh computers—tray-loading iMac computers and Power Macintosh G3 (blue and white) computers—require static addressing when using NetBoot. See “Network Requirements” on page 488.

Client computer RAM requirements

The following are the minimum RAM requirements for a client computer starting up from a Mac OS 9 or Mac OS X NetBoot disk image.

Start up from Mac OS 9 disk image: 64 MB

Start up from Mac OS X disk image: 128 MB

Client computers using Network Install must also have 128 MB of RAM.

Software updates for NetBoot system disk images

You should make sure to use the latest system software available when creating NetBoot disk images. New releases of Macintosh computers require updates of system software, so if you have new Macintosh clients you’ll need to update the disk images.

You cannot update Mac OS X disk images directly. To “update” your Mac OS X disk images, you must create new ones. See “Creating a Mac OS X Disk Image” on page 496.

To update Mac OS 9 disk images, see “Modifying the Mac OS 9 Disk Image” on page 498.

Ethernet support on client computers

NetBoot is supported only over the built-in Ethernet connection. Multiple Ethernet ports are not supported on client computers.

Network Requirements

The recommended method of provided IP addressing for NetBoot clients is DHCP. However, some older client computers require BootP for IP address assignment when using NetBoot. When this is the case, there can be only one server providing BootP addressing on the network to which those clients are attached. See the following section, “Capacity Planning,” for more information on this topic and other issues relevant to your network configuration when using NetBoot.

The following Macintosh computers require BootP addressing for NetBoot:

- tray-loading iMac computers
- Power Macintosh G3 (blue and white) computers

Capacity Planning

The number of NetBoot client computers you can connect to your server depends on how your server is configured, the server’s hard disk space, and a number of other factors.

In planning for your server and network needs, consider these factors:

- *Ethernet speed:* 100Base-T or faster connections are required for both client computers and the server. As you add more clients, you may need to increase the speed of your server’s Ethernet connections. Ideally you want to take advantage of the Gigabit Ethernet capacity built in to your Mac OS X server hardware to connect to a Gigabit switch. From the switch you should connect Gigabit Ethernet or 100 Mb Ethernet to each of the NetBoot clients.
- *Hard disk capacity and number of NetBoot images:* The NetBoot server requires a certain amount of hard disk space depending on the size and configuration of the system image and the number of images being served.
- *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. Because the system software for a disk image is written to a shadow image for each client booting from the disk image, you can get a rough estimate for the required hard disk capacity required by multiplying the size of the shadow image by the number of clients.

- *Location of server and client:* NetBoot clients that require static IP addresses (NetBoot 1.0) must be located on the same subnet as the server, and there can be only one server on that subnet serving static addresses.
- *Number of Ethernet ports on the switch:* Distributing NetBoot clients over multiple Ethernet ports on your switch offers a performance advantage. Each port must serve a distinct segment.

NetBoot Implementation

This section describes how NetBoot is implemented on Mac OS X Server—including information on the protocols, files, directory structures, and configuration details that support the NetBoot functionality.

NetBoot Image Folder

The *NetBoot image folder* contains the startup disk image file, a boot file that the firmware uses to begin the startup process, and other files required to start up a client computer over the network. A NetBoot image folder (NBI folder) is something like a package file (a folder compressed into a file), except that the folder and its contents are uncompressed so that the contents are readily visible. The name of a NetBoot image folder includes the suffix “.nbi”.

An NBI folder for Mac OS 9 (MacOS 9.2.2.nbi) is slightly different from an NBI folder for Mac OS X (MacOSX.nbi) since the components required for startup are different. The following tables describe the contents of each.

Mac OS X NetBoot image folder (MacOSX.nbi)

File	Description
booter	Boot file
mach.macos.x	UNIX kernel
mach.macosx.mkext	Drivers
MacOSX.dmg	System startup image file (may include application software)
NBImageInfo.plist	Property list file

You use Network Image Utility to create a Mac OS X NBI folder. The utility lets you

- name the image
- choose the image type (NetBoot or Network Install)
- provide an image ID (not visible to users)
- choose the default language—English, French, German, or Japanese
- specify a default user name and password

- enable automatic installation (Network Install only)
- add additional package or preinstalled applications (Network Install only)

Note: The size of the disk image is set automatically by Network Image Utility when you choose the image type. NetBoot disk images are 2.0 GB and Network Install disk images are 1.4 GB.

See “Creating a Mac OS X Disk Image” on page 496.

Mac OS 9 NetBoot image folder (MacOS9.2.2.nbi)

File or Folder	Description
Mac OS ROM	Boot file
NetBoot HD.img	System startup image file
Application HD.img	Application image file
NBImageInfo.plist	Property list file
Backup	Folder created by NetBoot Desktop Admin for the backup image

You use NetBoot Desktop Admin to modify the Mac OS 9 NBI folder. The utility lets you change the image file (NetBoot HD.img), the name of the image, adjust the size of the image, and add software to the application image.

Property List File

The property list file (NBImageInfo.plist) stores the properties that you use to configure an NBI folder. The property lists for Mac OS 9 and Mac OS X are described in the following tables. For the most part, the values in the NBImageInfo.plist are set by the tools you use to work with the image files—NetBoot Desktop Admin (for Mac OS 9 images) and Network Image Utility (for Mac OS X images)—and you do not need to change the property list file directly. Some values are set by the Configure DHCP/NetBoot panel in Server Settings. If you need to edit a property list file, however, you can use PropertyListEditor, which is supplied on the *Mac OS X Server Administration Tools* CD.

Mac OS 9 property list

Property	Type	Description
BootFile	String	Name of boot ROM file: Mac OS ROM.
Index	Number	Image ID.
IsDefault	Boolean	True specifies this image file as the default.

Property	Type	Description
IsEnabled	Boolean	Sets whether the image is available to NetBoot (or Network Image) clients.
IsInstall	Boolean	True specifies a Network Install image; False specifies a NetBoot image.
Name	String	Name of the image as it appears in the Startup Disk control panel (Mac OS 9) or Preferences pane (Mac OS X).
Type	String	Classic.

Mac OS X property list

Property	Type	Description
BootFile	String	Name of boot ROM file: booter.
Index	Number	Image ID.
IsDefault	Boolean	True specifies this image file as the default.
IsEnabled	Boolean	Sets whether the image is available to NetBoot (or Network Image) clients.
IsInstall	Boolean	True specifies a Network Install image; False specifies a NetBoot image.
Name	String	Name of the image as it appears in the Startup Disk control panel (Mac OS 9) or Preferences pane (Mac OS X).
RootPath	String	Specifies path to disk image on server.
Type	String	NFS.

Boot Server Discovery Protocol (BSDP)

NetBoot uses an Apple-created extension to BootP and DHCP called Boot Server Discovery Protocol, or BSDP for short. This protocol implements a method of discovering NetBoot servers on a network. BSDP allows NetBoot clients to obtain their IP identities from either the BSDP server or from a DHCP server elsewhere on the network. BSDP provides some basic load balancing. See “Load Balancing” on page 504.

TFTP and the Boot ROM File

NetBoot uses the Trivial File Transfer Protocol (TFTP) to send the boot ROM from the server to the client. Installation of the NetBoot software on a server places the Mac OS 9 boot ROM file in `/Library/NetBoot/NetBootSPx/imagename.nbi/` (where *x* is the volume number and *imagename* is the name of the NBI folder.) The file is called “Mac OS ROM.” For Mac OS X images, Network Image Utility creates the boot ROM file (“booter”) at this location. The NetBootSPx directory is automatically created as an NFS share point when you install NetBoot on your server.

Instead of pointing the client directly to the location of the boot ROM file, NetBoot points to a symbolic link stored in the directory `/private/tftpboot/`. The symbolic link references the actual location of the Mac OS ROM file. This allows you to move the Mac OS ROM file, should the need arise, by changing the symbolic link in `/private/tftpboot/`.

Disk Images

The read-only disk images contain the system software and applications used over the network by the client computers. The name of a disk image file typically ends in `.img` or `.dmg`. Disk Copy—a utility included with Mac OS X and Mac OS 9.2.2—can mount disk image files as volumes on the desktop. With NetBoot, disk images mounted this way behave as system startup disks.

You set up Mac OS 9 and Mac OS X disk images in slightly different ways. A preconfigured Mac OS 9 disk image is provided for you on the CD named *NetBoot, Mac OS 9*. (The CD contains four localized versions of the Mac OS 9 image: Tier 0: English, Japanese, French, and German.) See “Installing the Mac OS 9 Disk Image” on page 497. You can modify the Mac OS 9 disk image using NetBoot Desktop Admin. See “Modifying the Mac OS 9 Disk Image” on page 498.

You use Network Image Utility to create Mac OS X disk images, using a Mac OS X install disc as the “source.” See “Creating a Mac OS X Disk Image” on page 496.

Shadow Images

Many clients may read from the same system disk image, but whenever a client needs to write anything back to its startup volume (such as print jobs and other temporary files), NetBoot automatically redirects the written data to the client’s *shadow image*—a file hidden from regular system and application software. The shadow image is what preserves the unique identity of each computer during the entire time it is running off a NetBoot server disk image. NetBoot transparently handles reading changed data from the shadow file, while reading unchanged data from the shared system image. The shadow image is recreated at boot time, so any changes made by the user to his or her startup volume are lost upon restart. For instance, if a user saves a document to the startup volume, after a restart that document will be gone. This behavior preserves the condition of the environment the administrator set up. Therefore it is recommended that users have accounts on a file server on the network to save their documents.

NetBoot creates share points on all available server volumes to store client shadow images as a way of providing load balancing for NetBoot clients. See “Load Balancing” on page 504.

NetBoot Files and Directory Structure

NetBoot learns about a client it supports the first time the client attempts to start up from the NetBoot server. When a client attempts to start up from a disk image on the NetBoot server, it provides information to NetBoot, which NetBoot saves and uses to identify the client during future startup attempts. The file that holds this information is called `bsdpd_client` and is kept in the `/var/db/` directory.

Security

You can secure access to NetBoot service on a case-by-case basis using the hardware address of specific computers to which you specifically allow or deny access. A client computer’s hardware address is automatically added to the NetBoot Filtering list when the client starts up using NetBoot and is, by default, enabled to use NetBoot. See “Filtering NetBoot Client Connections” on page 503.

Note: The hardware address for a computer using Mac OS X can be found by opening the Network system preference and examining the Ethernet address under TCP/IP. The hardware address for a computer using Mac OS 9 can be found by opening the TCP/IP control panel, choosing Get Info from the File menu, and examining the hardware address.

NetBoot and AirPort

The use of AirPort wireless technology with NetBoot clients is *not* supported by Apple and is discouraged.

Setup Overview

Here is an overview of the basic steps for setting up NetBoot:

Step 1: Evaluate and update your network, servers, and client computers as necessary

The number of client computers you can support using NetBoot is determined by the number of servers you have, how they are configured, hard disk storage capacity, and other factors. See “Capacity Planning” on page 488.

Some older client computers require BootP for getting an IP address assignment when using NetBoot. (See “Network Requirements” on page 488 for a list of Macintosh computers that require BootP.) When this is the case, you must make sure that only one server on the network to which those clients are attached is configured to supply BootP addressing. Because this may impact your ability to implement a load balancing strategy, you may want to set up a separate subnet for these clients, as described in the next step. For more information about providing load balancing for NetBoot clients see “Load Balancing” on page 504.

Depending on the results of your evaluation in step 1, you may want to add servers or hard disks, add Ethernet ports, or make other changes to your servers, and you may want to set up one or more subnets for your BootP clients, depending on the number of BootP clients that you have.

You may also want to implement subnets on this server (or other servers) in order to take advantage of NetBoot filtering. See “Filtering NetBoot Client Connections” on page 503.

If you plan to provide personalized work environments for NetBoot clients by using Workgroup Manager (Mac OS X clients) and Macintosh Manager (Mac OS 9 clients), you should set this up and import users from the Mac OS X Server Users & Groups database before you create disk images. Make sure you have at least one Macintosh Manager user assigned to the System Access workgroup for Mac OS 9 clients and the Workgroup Manager for Mac OS X clients. See Chapter 6, “Client Management: Mac OS X,” on page 267 and Chapter 10, “Client Management: Mac OS 9 and OS 8,” on page 411.

If you plan to provide authentication and personalized work environments for NetBoot client users by using Workgroup Manager (Mac OS X clients) and Macintosh Manager (Mac OS 9 clients), you should set this up and import users from the Mac OS X Server Users & Groups database before you create disk images. Make sure you have at least one Macintosh Manager user assigned to the System Access workgroup for Mac OS 9 clients and the Workgroup Manager for Mac OS X clients. See Chapter 6, “Client Management: Mac OS X,” and Chapter 10, “Client Management: Mac OS 9 and OS 8.”

Step 2: Create disk images for client computers

You can set up both Mac OS 9 disk images and Mac OS X disk images for client computers to start up from. A preconfigured Mac OS 9 image is supplied with Mac OS X Server on the *NetBoot, Mac OS 9* CD. The Mac OS 9 disk image can be modified. If you are supporting new client computers that were released after this version of Mac OS X Server, you will need to modify the Mac OS 9 disk image to support the new clients. See “Modifying the Mac OS 9 Disk Image” on page 498.

To create Mac OS X disk images, you use Network Image Utility. See “Creating a Mac OS X Disk Image” on page 496.

Step 3: Set up DHCP

NetBoot requires that you have a DHCP—either on the local server or on a remote server on the network. You need to make sure that you have a range of IP addresses sufficient to accommodate the number of clients that will be using NetBoot at the same time.

See Chapter 11, “DHCP Service,” on page 475.

Step 4: Configure and turn on the NetBoot service

You use the Configure DHCP/NetBoot panel in Server Settings to configure NetBoot on your server. See “Configuring NetBoot on Your Server” on page 501.

You turn on the NetBoot service by starting DHCP/NetBoot service and enabling disk images. See “Starting NetBoot on Your Server” on page 501 and “Enabling NetBoot Disk Images” on page 502.

Step 5: Set up NetBoot filtering (optional)

NetBoot filtering is done by client computer hardware address. Each client’s hardware address is automatically registered the first time the client attempts to start up from a NetBoot disk image. You then disallow a client address to prevent the client from using NetBoot. See “Filtering NetBoot Client Connections” on page 503.

Step 6: Test your NetBoot setup

Because there is risk of data loss or bringing down the network (by misconfiguring DHCP), it is recommended that you test your NetBoot setup before implementing it on all your clients. You should test each different model of Macintosh that you are supporting. This is to make sure that there are no problems with the boot ROM for a particular hardware type.

Step 7: Set up all client computers to use NetBoot

When you are satisfied that NetBoot is working on all types of computers then you can set up all your client computers to start up from the NetBoot disk images.

You can set up NetBoot in the following ways:

Clients running Mac OS 9: Use the Startup Disk control panel to select a startup disk image on the server, then restart the computer. See “Selecting a NetBoot Startup Image (from Mac OS 9)” on page 506.

Note: You must update the Startup Disk control panel on client computers running Mac OS 9 from their local hard disks in order to be able to view NetBoot disk images in the control panel. See “Updating the Startup Disk Control Panel” on page 505.

Clients running Mac OS X version 10.2 or later: Use the Startup Disk System Preference pane to select a startup disk image on the server, then restart the computer. See “Selecting a NetBoot Startup Image (from Mac OS X)” on page 506.

Any client: Restart the computer and hold down the N key until the NetBoot icon starts flashing on the screen. The client starts up from the default image on the NetBoot server. See “Starting Up Using the N Key” on page 507.

Setting Up NetBoot on a Mac OS X Server

This section describes how to enable NetBoot on a Mac OS X server and how to create and edit NetBoot disk images.

Creating a Mac OS X Disk Image

NetBoot lets you provide one or more Mac OS X disk images to support NetBoot clients you want to start up over the network. You use Network Image Utility to create these images.

Network Image Utility creates a Mac OS X disk image by using the files on a Mac OS X installation disc. Have the install CD ready—you’ll need to insert the disc into the CD drive during this procedure.

Note: You are required to purchase a user license for each client starting up from a NetBoot disk image.

To create a Mac OS X disk image:

- 1 Open Network Image Utility.
- 2 Enter a name for the disk image you are creating.
- 3 Select NetBoot from the Image Type popup menu.

Network Image Utility automatically adjusts the size of the disk image depending on the type of image you create. NetBoot disk images are 2 GB and Network Install disk images are 1.4 GB.

- 4 Enter an Image ID.

The Image ID allows you mount multiple identical disk images (on multiple servers) without each of them showing up in clients’ Startup Disk control panels and panes. All the images with the same image name and ID are listed only once. Providing duplicate disk images on multiple servers allows Mac OS X Server to employ load balancing for NetBoot clients.

- 5 Choose the default language for the system: English, French, German, or Japanese.
- 6 (Optional) Enter the default user name, short name, and password (in both the Password and Verify fields) to create a default user account.

Entering a default name and password creates a “dummy” user account that anyone can use to log in to the disk image. Users who have their own accounts can also log in with their own names and passwords. The default user is created with administrator privileges for the client computer.

- 7 Click Create Image.

If you haven't inserted a Mac OS X install CD, you will be prompted to do so.

The image file is created and saved in a NetBoot image folder in the following location, where *x* is the volume number and *imagename* is the image name you provided:

```
/Library/NetBoot/NetBootSPx/imagename.nbi/
```

If the source for the Mac OS X software is on two CDs, you will be prompted to remove the first disc and insert the second.

Installing Classic (Mac OS 9) on a Mac OS X Disk Image

You install Classic onto a Mac OS X image by copying a Mac OS 9.2.2 system folder onto an “unlocked” NetBoot image. You must also select the Mac OS X image and start Classic using the System 9 preference pane to complete the integration of Classic into the image.

Do not try to install Classic onto Network Install disk images. This procedure for installing Classic only works for NetBoot disk images.

Warning Do not modify a disk image that is in use by any NetBoot clients. Doing so will result in unpredictable behavior for the clients. Before modifying a disk image, make sure no one is using the image or make a copy of the file and modify the copy.

To install Classic on a Mac OS X disk image:

- 1 Make sure the disk image file (.dmg) is unlocked.
In the Finder, select the image file and choose Show Info from the File menu. If the file is locked, click the Locked checkbox to unlock it.
- 2 Double-click the image file to mount the Mac OS X image on your server.
- 3 Drag a Mac OS 9 System Folder to the disk image.
You can use the System Folder from the *NetBoot, Mac OS 9* CD that came with Mac OS X Server, or use another Mac OS 9 version 9.2.2 System Folder that has been blessed (previously run as Classic under Mac OS X.)
- 4 In your server's System Preferences, open the Classic preferences pane and select the disk image as the startup volume for Classic.
- 5 Click Start to start up Classic.
- 6 Shut down Classic, then eject the image file.
- 7 (optional) Lock the image file if you want to protect against inadvertent changes.

Installing the Mac OS 9 Disk Image

Included with the NetBoot software is a preconfigured Mac OS 9 disk image, provided on the *NetBoot, Mac OS 9* CD, which you install from the NetBoot.pkg file.

To install the preconfigured Mac OS 9 disk image:

- Open NetBoot.pkg on the *NetBoot, Mac OS 9* CD.

The Installer installs the Mac OS 9 NetBoot image folder in the `/Library/NetBoot/NetBootSPx/DefaultMacOS92.nbi/` directory (where *x* is the volume number).

Modifying the Mac OS 9 Disk Image

To install software on or change the preconfigured Mac OS 9 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).

The following procedure requires that you restart the client computer several times.

Important Be careful if there is more than one NetBoot server on your network. The client may start up automatically from a disk image on a server other than the one you are working on.

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.

- 1** Log in to the server volume as a user with read and write access privileges (for example, as an administrator of the Mac OS X Server).
- 2** Using the Chooser, log in to all the server volumes on the client.
- 3** Copy the NetBoot Desktop Admin application to your server hard disk then open the application.

NetBoot Desktop Admin is supplied on the *NetBoot, Mac OS 9* CD.

- 4** 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.

- 5 If you are installing a new version of the Mac OS or adding system extensions, you may need to increase the size of the disk image.

Make sure the disk image is large enough to accommodate the size of the new system and extensions you are installing. You cannot reduce the size of an image without reverting to a smaller backup copy.

- 6 If you are installing a new application software, you may need to increase the size of the application disk image.

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 smaller backup copy.

- 7 Install the software or make changes to the system configuration.

Make sure to install the latest updates for the system software.

If you are installing software, follow the installation instructions that came with the software. If necessary, restart the computer.

After installing 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.

- 8 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.

- 9 User the Chooser, log back in to all the server volumes.

- 10 Open the NetBoot Desktop Admin application, then click Save. The computer restarts automatically.

If you need to make other changes, click Quit and return to Step 7.

Clicking Discard removes the changes you've made to the disk image.

- 11 Start the NetBoot client computer again, and log back in to all the server volumes.
- 12 Open NetBoot Desktop Admin.

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.

Note: Because there is only one Backup folder, the backup image saved at this time will overwrite any backup image in the folder from a previous session.

- 13 If you clicked Save in Step 10, click Restart. Otherwise, click OK.

If you click Restart, NetBoot Desktop Admin saves your changes, deletes the old disk image, and 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.

Specifying the Default NetBoot Disk Image

The *default disk image* is the NetBoot disk image used when a user starts a client computer using the N key. See “Starting Up Using the N Key” on page 507. If you've created more than one startup disk image, use the Configure DHCP/NetBoot pane to select the default startup image.

Note: If you have more than one NetBoot server on the network, there is no way to control which disk image is used by client computers looking for the default disk image. The default image of the first server to respond to the client's NetBoot request is the one that will be used.

To specify the default NetBoot disk image:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3 Click the Image tab.
- 4 Select the image you want to be the default.

Setting Up Multiple Disk Images

You can create as many Mac OS X disk images as you want using the Network Image Utility. To create more than one Mac OS 9 disk image, make copies of the preconfigured disk image you installed from the *NetBoot, Mac OS 9* CD into the `/Library/NetBoot/NetBootSP0` directory. Then use NetBoot Desktop Admin to modify the Mac OS 9 disk images as desired.

Use Server Settings to enable disk images and select the default disk image. See “Enabling NetBoot Disk Images” on page 502 and “Specifying the Default NetBoot Disk Image” on page 500.

Configuring NetBoot on Your Server

You use DHCP/NetBoot module of Server Settings to configure your Mac OS X Server to provide NetBoot services to client computers.

Note: In the previous release of Mac OS X Server, “Static” was referred to as NB 1.0 and “Dynamic” as NB 2.0.

To configure NetBoot:

- 1 Open Server Settings and click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3 Click the Logging tab and choose the level of logging you want: “Warning and errors (normal)” or “Serious errors only (quiet).”
- 4 Click the NetBoot tab and select an Ethernet port to use for NetBoot.
You can select multiple ports to configure them simultaneously.
- 5 Select Static, Dynamic, or both.

“Static” provides NetBoot service for NetBoot 1.0 clients.

“Dynamic” provides NetBoot service for NetBoot 2.0 and NetBoot 3.0 clients.

Important Make sure that you set up only one static server on a network. Setting up multiple static servers may prevent NetBoot 1.0 clients from being able to start up over the network.

If you chose Dynamic and have an existing DHCP infrastructure, skip the following four steps and continue with Step 10.

- 6 For each Ethernet port you want to set up for NetBoot, repeat step 5.
- 7 If you chose Static or Both, click the Subnets tab and choose the matching port name.
- 8 Click Edit, then create an IP address range for the port. Make sure that the Enable DHCP option is selected.
- 9 Repeat Steps 7 and 8 for each port over which you’re serving NetBoot.
- 10 Click the Image tab.

Select the Enable checkbox of the images that you want to make available to client computers for startup, then click Apply Now.

Starting NetBoot on Your Server

You turn on NetBoot by starting DHCP.

Note: You must also enable one or more images on your server before client computers can use NetBoot.

To start DHCP:

- 1 Open Server Settings and click the Network tab.
- 2 Click DHCP/NetBoot and choose Start DHCP Service.

Enabling NetBoot Disk Images

You must enable one or more disk images on your server to make the images available to client computers for NetBoot startups.

Note: You must also start DHCP on the server before client computers can use NetBoot.

To enable disk images:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3 Click the Image tab.
- 4 Select the Enable checkbox for the images you want to make available for NetBoot clients.

Managing NetBoot

This section describes how to manage the ongoing use of a NetBoot installation.

Turning Off NetBoot

The best way to prevent clients from using NetBoot on the server is to disable NetBoot service on all Ethernet ports.

Note: You can also stop NetBoot by disabling all disk images on the server.

To disable NetBoot on Ethernet ports:

- 1 Open Server Settings and click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3 Click the NetBoot tab and make sure no Ethernet ports are selected.

Disabling Disk Images

Disabling a disk image prevents client computers from using the image to start up over the network.

To disable a NetBoot disk image:

- 1 In Server Settings, click the Network tab.
- 2 Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3 Click the Image tab.

- 4 Select an image and deselect the Enable checkbox.

Updating Mac OS X Disk Images

Because Network Image Utility works by creating disk images from installation files on a CD-ROM disc, you cannot update a Mac OS X disk image. You must create a new disk image using a current Mac OS X installation CD.

Monitoring the Status of Mac OS X NetBoot Clients

Server Status lets you monitor all services on a Mac OS X server.

To monitor NetBoot service:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select DHCP/NetBoot in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Overview tab to see if DHCP/NetBoot is running.
- 3 Click the NetBoot Clients tab to see a list of client computers that have started up from the server, the hardware addresses of the clients, and the clients' system type.

Note: This is historical information—a list of clients that are currently connected or have connected in the past. It is not a list of currently connected clients only.

Monitoring the Status of Mac OS 9 NetBoot Clients

Server Status lets you monitor all services on a Mac OS X server.

To monitor NetBoot service:

- 1 In Server Status, locate the name of the server you want to monitor in the Devices & Services list and select AppleFile in the list of services under the server name.
If the services aren't visible, click the arrow to the left of the server name.
- 2 Click the Overview tab to see if DHCP/NetBoot is running.
- 3 Click the Connections tab to see a list of client computers currently connected to the server, their types, IP addresses, how long the computers have been connected, and how long the computers have been idle.

Filtering NetBoot Client Connections

The filtering feature of NetBoot lets you allow or deny NetBoot access by client computer hardware addresses. Client hardware addresses are added to the filter list automatically the first time clients start up from a NetBoot disk image and are allowed access by default, so it is usually not necessary to enter hardware addresses manually.

To allow or deny client access to the NetBoot service:

- 1** Open Server Settings and click the Network tab.
- 2** Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3** Click the Filter tab.
- 4** Select the clients you want to allow access and which you want to deny access to the NetBoot service.

Load Balancing

NetBoot provides a significant benefit to those system administrators tasked with maintaining a large number of Macintosh computers by having all of those computers boot from the same system software image. This feature, however, makes it critical that the NetBoot server remain available to the client computer relying upon it. To provide responsive and reliable NetBoot service, you should set up redundant NetBoot servers in your network infrastructure.

Most sites using NetBoot achieve acceptable responsiveness by staggering the boot times of client computers in order to reduce network load. Generally, there isn't a need to boot all client computers at exactly the same time; rather, client computers are booted early in the morning and just remain booted throughout the work day. For clients computers running Mac OS 9, you can program staggered startup times using the Energy Saver control panel. (There is no equivalent feature in Mac OS X, however.)

If heavy usage and simultaneous client startups are overloading the NetBoot server and causing delays, you may want to consider adding additional NetBoot servers to distribute the demands of the client computers across multiple servers (*load balancing*). When incorporating multiple NetBoot servers, it is important to use switches, as the shared nature of hubs creates a single shared network on which additional servers would have to vie for time.

Enabling Server Selection

If you add a second NetBoot server to a network that has a single server already in use, you will need to delete the `bsdnpd_clients` file (located in the directory path `/var/db/`) from the existing NetBoot server. This enables clients to select which server they will use as their NetBoot server. Similarly, if you are recovering from a server or infrastructure failure, and your clients have been booting from a reduced number of NetBoot servers, you will need to delete the `bsdnpd_clients` file from the running servers so that clients can once again spread out across the entire set of servers.

The `bsdpd_clients` file on any given server holds the Ethernet Media Access Control (MAC) addresses of the machines that have selected this server as their NetBoot server. As long as a client has an entry in an available server `bsdpd_client` file, it will always boot from that server. If that server should become unavailable to those clients, they will locate and associate themselves with an available server until such time as you remove their entries (or the entire files) from their servers. (If a client ends up being registered on more than one server because an unavailable server comes back on line, the client boots from the server with the fewest number of clients booted off of it.)

Using Share Points to Spread the Load

By default, NetBoot creates share points for client shadow images on all server volumes in order to spread the load across multiple drive mechanisms. You can use Workgroup Manager to see these share points. They are named `NetBootSPx` where *x* is the share point number—the share points are numbered starting with zero. For instance, if your server has two volumes installed (`NetBootSP0` and `NetBootSP1`), NetBoot stores the first client's shadow image on `NetBootSP0`, the second client's shadow image on `NetBootSP1`, the third client's shadow image on `NetBootSP0`, and so on. Likewise, with three volumes installed and eight clients, the first, fourth, and seventh clients will use the first volume; the second, fifth, and eighth clients will use the second volume; and the third and sixth clients will use the third volume. This load balancing is automatic and usually ensures optimal performance.

With drive sizes getting larger and larger, some sites elect to partition their drives. An example would be partitioning a 60GB drive into a 10GB boot partition and a 50GB data partition, with the intention of keeping just your operating system and associated configuration files on the boot partition, and all user data (such as client shadow images) on the data partition. After installation of the NetBoot software, however, there will be a `NetBootSP0` on the boot partition and a `NetBootSP1` on the data partition.

Supporting Client Computers

See “Client Computer Requirements” on page 487 for a list of supported Macintosh computers and the client system requirements for using NetBoot.

Updating the Startup Disk Control Panel

You need to replace the Startup Disk control panel for client computers running Mac OS 9 in order for the control panel to be able to display the available NetBoot disk images.

Version 9.2.4 of the Startup Disk control panel is located on the *NetBoot, Mac OS 9* CD.

- Drag the new version of the control panel to the System Folder of each client computer running Mac OS 9 locally.

Setting Up “System-Less” Clients

NetBoot makes it possible to configure client computers without locally installed operating systems. “System-less” clients can start up from a NetBoot server using the N key method. (See “Starting Up Using the N Key” on page 507.)

After the client computer has started up, you can use the Startup Disk control panel (Mac OS 9) or preference pane (Mac OS X) to select the NetBoot disk images as the default startup disk for the client. That way you no longer need to use the N key method to start up the client from the server.

Removing the system software from client computers gives you additional control over users’ environments. By forcing the client to boot from the server and using client management to deny access to the client computer’s local hard disk, you can prevent users from saving files to the local hard disk.

Selecting a NetBoot Startup Image (from Mac OS X)

If your computer is running Mac OS X version 10.2 or later, you use the Startup Disk System Preferences pane to select a NetBoot startup disk image.

To select a NetBoot startup image from Mac OS X:

- 1 In System Preferences select the Startup Disk pane.
- 2 Select the network disk image you want to use to start up the computer.
- 3 Click Restart.

The NetBoot icon appears, and then the computer starts up from the selected NetBoot disk image.

Selecting a NetBoot Startup Image (from Mac OS 9)

If your computer is running Mac OS 9, you use the Startup Disk control panel to select a NetBoot startup disk image.

Note: You must update the Startup Disk control panel on client computers running Mac OS 9 from their local hard disks in order to be able to view NetBoot disk images in the control panel. See “Updating the Startup Disk Control Panel” on page 505.

To select a NetBoot startup image from Mac OS 9:

- 1 Open the Startup Disk control panel.
- 2 Select the network disk image you want to use to start up the computer.
- 3 Click Restart in the warning dialog box that appears.

The NetBoot icon appears, and then the computer starts up from the selected NetBoot disk image.

The network disk image appears with a distinctive icon.

Starting Up Using the N Key

You can use this method to start up any supported client computer from a NetBoot disk image. When you start up with the N key, the client computer starts up from the default NetBoot disk image. (If there are multiple servers present, then the client starts up from the default image of the first server to respond.)

If you have an older client computer that requires BootP for IP addressing, you must use this method for starting up from a NetBoot disk image. These older computers do not support selecting a NetBoot startup disk image from the Startup Disk control panel or preferences pane.

The N key also provides a way to start up client computers running Mac OS 8 or that do not have system software installed. See “Setting Up “System-Less” Clients” on page 506.

To start up from a NetBoot disk image using the N key:

- 1 Turn on (or restart) your computer while holding the N key down on your keyboard.
Hold the N key down until the NetBoot icon appears in the center of the screen or an arrow appears in the upper left corner of the screen.
- 2 If a login window appears, enter your name and password.
The network disk image has an icon typical of server volumes.

Solving Problems

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.
- 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 to which the client computer is connected. 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.

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 on which the user does not have an account. 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 Install

Network Install lets you install Mac OS X system and other software onto client computers over the network. Network Install is similar to NetBoot. Instead of using start-up disk images on the server, however, client computers start up from installer disk images. An *installer disk image* looks and behaves like an installer CD. Client computers can start up from the installer disk image on Mac OS X server. After a client has started up, system software, application software, or both can be installed on the client. Installations can be set up to run unattended (“automated”) or to require user interaction, allowing users to specify installation options.

Note: Network Install only installs Mac OS X system software on client computers. You cannot use Network Install to install Mac OS 9.

If you haven’t done so already, read Chapter 12, “NetBoot,” before continuing. In addition to describing how NetBoot works, Chapter 12 includes important prerequisites for anyone attempting to use NetBoot or Network Install.

You use the following Mac OS X Server applications to set up and administer Network Install:

- *Network Image Utility*—to create Mac OS X installer disk images.
- *Package Maker*—to create package files that can be included on disk images.
- *PropertyListEditor*—to edit property list (.plist) files to include packages in an installer disk image.

The Mac OS X Server product includes the following CD that contains applications you use to set up Network Install:

- *Mac OS X Server Administration Tools* CD
 - NetBoot, Network Install *f*—includes Network Image Utility (in Image Creation *f*) and Package Maker and PropertyListEditor (in Image Manipulation *f*)

Understanding Packages

If you plan to use Network Install to install application software, you need to know what packages are and how they work.

A *package* is a collection of compressed files and other information used to install software onto a computer. The contents of a package are contained within a single file, which has the extension .pkg. The following table shows the components of a package file.

File	Description
product.pax.gz	The files to be installed, compressed with gzip and archived with pax. (See man pages for more information about gzip and pax.)
product.bom	Bill of Materials: a record of where files are to be installed. This is used in the verification and uninstall processes.
product.info	Contains information to be displayed during installation.
product.sizes	Text file; contains the number of files in the package.
product.tiff	Contains custom icon for the package.
product.status	Created during the installation, this file will either say “installed” or “compressed.”
product.location	Shows location where the package will be installed.
software_version	(Optional) Contains the version of the package to be installed.

The contents of a package can be viewed by selecting the package and holding down the Command, Shift, and O keys. This opens a viewer window in which the contents of the package are displayed.

You use Package Maker, available on the *Mac OS X Server Administration Tools* CD, to create application software packages to use with Network Install. Additional information about Package Maker is available at the following Web site:

<http://developer.apple.com/techpubs/macosx/DeveloperTools/PackageMaker/PackageMaker.help/Contents/Resources/English.Iproj/>

Setup Overview

Here are the basic steps for creating installer disk images.

Step 1: Read the NetBoot chapter and enable NetBoot on your server

Chapter 12, “NetBoot,” provides important information, such as system requirements and configuration procedures that you’ll need to know to use Network Install. Follow the instructions in “Starting NetBoot on Your Server” on page 501 to turn on NetBoot and Network Install.

Step 2: Create a Mac OS X installer disk image

Use Network Image Utility to create one or more Mac OS X installer images. See “Creating a Network Install Disk Image” on page 511.

Step 3: (Optional) Create an application software package

Use Package Maker to create packages if you want to install application software over the network. Application software packages can be used by themselves or in conjunction with Mac OS X system software. See “Creating Custom Packages for Network Install” on page 512. To include the packages in an installer disk image you must edit the image’s property list (.plist) file using PropertyListEditor. See “Including Packages in an Installer Disk Image” on page 512.

Step 4: Enable installer disk images on your server

You enable installer disk images in the DHCP/NetBoot pane in Server Settings. See “Enabling Installer Disk Images” on page 513.

Setting Up Network Install

This section tells you how to create network installer disk images and enable them on your server.

Creating a Network Install Disk Image

You use Network Image Utility to create installer disk images. Network Image Utility is included with the Mac OS X Server product on the *Mac OS X Server Administration Tools* CD, at the following location:

NetBoot, Network Install *f*/ImageManipulation *f*

Network Image Utility creates an installer disk image by using the files on a Mac OS X install disc. Have the install CD ready—you’ll need to insert the disc into the CD drive during this procedure.

To create a Mac OS X installer disk image:

- 1** Open Network Image Utility.
- 2** Enter a name for the disk image you are creating.
- 3** Select Network Install from the Image Type pop-up menu.

To create an image for installing application software packages only (no system software), choose Empty Image from the Image Type pop-up menu.

Network Image Utility automatically adjusts the size of the disk image depending on the type of image you create. NetBoot disk images are 2 GB and Network Install disk images are 1.4 GB.

- 4 Enter an Image ID.

The Image ID lets you mount multiple identical disk images (on multiple servers) without each of them showing up in a client's Startup Disk control panel or pane. All the images with the same image name and ID will be listed only once.

- 5 Choose the default language for the system: English, French, German, or Japanese.
- 6 (Optional) Enter the default user name, short name, and password (in both the Password and Verify fields) to create a default user account.

Entering a default name and password creates a user account that anyone can use to log in to the disk image. Users that have their own accounts can also log in with their own names and passwords. The default user is created with administrator privileges for the client computer.

- 7 Click Create Image.

If you haven't inserted a Mac OS X installer CD, you will be prompted to do so.

The image file is created and saved in a NetBoot image folder in the following location, where *x* is the volume number and *imagename* is the Image Name you provided:

```
/Library/NetBoot/NetBootSPx/imagename.nbi/
```

Creating Custom Packages for Network Install

You can use Package Maker to create additional packages to include with an installer disk image. Package Maker is included with the Mac OS X Server product on the *Mac OS X Server Administration Tools* CD, at the following location:

```
NetBoot, Network Install f/ImageManipulation f
```

Use PropertyListEditor to update the property list file to include your custom packages. See "Including Packages in an Installer Disk Image" on page 512.

Including Packages in an Installer Disk Image

Use PropertyListEditor to update the property list (.plist) file of the installer disk image to include packages with the installer. PropertyListEditor is included with the Mac OS X Server product on the *Mac OS X Server Administration Tools* CD, at the following location:

```
NetBoot, Network Install f/ImageManipulation f
```

To update the property list to include packages in an installer disk image:

- 1 Make sure the disk image file (.dmg) is unlocked.

In the Finder, select the image file and choose Show Info from the File menu. If the file is locked, click the Locked checkbox to unlock it.

- 2 Double-click the image file to mount the Mac OS X image on your server.

- 3 On the volume that gets mounted, Control-click the OSInstall.mpkg file at the following location:
volume/System/Installation/Packages/
- 4 Choose Show Package Contents to open a viewer window showing the package's contents.
- 5 Double-click the Contents folder, then double-click the Resources folder.
- 6 Open the Packages.plist.
PropertyListEditor should open. If not, open PropertyListEditor and open the property list file from within the application.
- 7 Create a new package in the Package list under Root.
- 8 Define the new package as a Dictionary using the Class pop-up menu.
- 9 Create a child labeled "packageName" of type String and enter the package name in the Value field.
- 10 Create a second child labeled "required" of type String and type YES in the Value field.
- 11 Repeat steps 7 through 10 for each package you want to add.
- 12 Save the updated property list and close PropertyListEditor.
- 13 In the Finder, copy the package files that correspond to the entries you just made in the property list into the following folder:
volume/System/Installation/Packages
- 14 Eject the image.
- 15 (Optional) Lock the image file if you want to protect against inadvertent changes.

Enabling Installer Disk Images

You must enable one or more of your installer disk images on your server to make the images available to client computers on the network.

You must also start DHCP on the server before client computers can use Network Install. See "Starting NetBoot on Your Server" on page 501.

Warning If an installer disk image is the only image you enable, it will become the default NetBoot image. Clients that start up using the N key will boot from and run the installer image instead of booting from a startup disk image.

To enable installer disk images:

- 1** In Server Settings, click the Network tab.
- 2** Click DHCP/NetBoot and choose Configure DHCP/NetBoot.
- 3** Click the Image tab.
- 4** Select the Enable checkbox for the images you want to make available for Network Install.

DNS Service

When your clients want to connect to a network resource such as a Web or file server, they typically request it by its domain name (such as `www.example.com`) rather than by its IP address (such as `192.168.12.12`). The Domain Name System (DNS) is a distributed database that maps IP addresses to domain names so your clients can find the resources by name rather than by numerical address.

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.

Setting up and maintaining a DNS server is a complex process. Therefore many administrators rely on their Internet service provider (ISP) for DNS services. In this case, you only have to configure your network preferences with the name server IP address provided by your ISP.

If you don't have an ISP to handle DNS requests for your network and either of the following is true, you need to set up DNS service:

- You do not have the option to use DNS from your ISP or other source.
- You plan on making frequent changes to the namespace and want to maintain it yourself.
- You have a mail server on your network and you have difficulties coordinating with the ISP that maintains your domain.

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.

Before You Set Up DNS Service

This section contains information you should consider before setting up DNS on your network. The issues involved with DNS administration are complex and numerous. You should only set up DNS service on your network if you are an experienced DNS administrator.

DNS and BIND

You should 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*, 4th edition, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 2001).

Note: Apple can help you locate a network consultant to implement your DNS service. You can contact Apple Professional Services and Apple Solutions Experts at:

<http://www.apple.com/services/>

<http://experts.apple.com/>

Setting Up Multiple Name Servers

You should set up at least one primary and one 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 periodically copying all the domain information from the primary server.

Once your name server learns a name/address pair of a host in another domain (outside the domain it serves), the information is cached, which ensures DNS services are available. DNS information is usually cached on your name server for a set time, referred to as a *time-to-live* (TTL) value. When the TTL for a domain name/IP address pair has expired, the entry is deleted from the name server's cache and your server will request the information again as needed. (The entry is never deleted from the domain owner's DNS server.)

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 that host is unavailable, 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 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 computer. 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.

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, the Internet Assigned Numbers Authority (IANA). IANA registration makes sure domain names are unique across the Internet. (See www.iana.org 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, a server in a domain would be `host1.example.com`, a server in a subdomain would be `host2.good.example.com`. The DNS server for `example.com` keeps track of information for its subdomains, such as host (or computer) names, static IP addresses, aliases, and mail exchangers.

The range of IP addresses for use with a given domain must be clearly defined before setup. These addresses are used exclusively for one specific domain (never by another domain or subdomain). The range of addresses should be coordinated with your network administrator or ISP.

Step 2: Configure BIND

BIND is the name of the program included with Mac OS X Server 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` is located in this directory:

```
/var/named/db.192.168.12
```

See “Inside DNS Service (Configuring BIND)” on page 520 for more information.

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

Mac OS X Server includes GUI tools to start and stop DNS service.

See “Starting and Stopping DNS Service” on page 518 for more information.

Managing DNS Service

Mac OS X Server provides a simple interface for starting and stopping DNS service as well as viewing logs and status. Changing DNS settings requires configuring BIND from the command line and is not covered here.

Starting and Stopping DNS Service

Use this procedure to start or stop DNS Service.

To start or stop DNS service:

- 1 In Server Settings, click the Network tab.
- 2 Click DNS Service and choose Start DNS or Stop DNS.

When the service is turned on, a globe appears on the DNS Service icon. The service may take a moment to start (or stop).

Viewing DNS Log Entries

DNS service creates entries in the system log for error and alert messages.

To see DNS log entries:

- 1 In Server Status, click the server name in the Devices and Services list.
- 2 Click the Logs tab.
- 3 Choose System Log from the Show pop-up menu and look for entries that begin with “named.”

Viewing DNS Service Status

You can check the DNS Status window to see

- whether the service is running
- the version of BIND (the underlying software for DNS) that is running
- when the service was started and stopped
- the number of zones allocated
- the number of transfers running and deferred
- whether the service is loading the configuration file
- if the service is priming
- whether query logging is turned on or off
- the number of Start of Authority (SOA) queries in progress

To view DNS service status:

- 1 In Server Status, click DNS in the Devices and Services list.
- 2 Click the Overview tab for general DNS service information.
- 3 Click the Activity tab to view operations currently in progress.

Viewing DNS Usage Statistics

You can check the DNS Statistics window to see statistics on common DNS queries.

- 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): Asks for text records used by the administrator.

To see DNS usage statistics:

- 1 In Server Status, click DNS in the Devices and Services list.
- 2 Click the Activity tab to view operations currently in progress and usage statistics.

Inside DNS Service (Configuring BIND)

In order to set up and use DNS service on Mac OS X Server you need to configure BIND. Configuring BIND requires making changes to UNIX configuration files in the Terminal application. To configure BIND, you must be comfortable with typing UNIX commands and using a UNIX text editor. Only manipulate these settings if you have a thorough understanding of DNS and BIND, preferably as an experienced DNS administrator.

Warning Incorrect BIND configurations can result in serious network problems.

What Is BIND?

As stated at the beginning of this chapter, BIND stands for Berkeley Internet Name Domain. BIND runs on UNIX-based operating systems and is distributed as open-source software. BIND is used on the majority of name servers on the Internet today.

BIND is configured by editing text files containing information about how you want BIND to behave and information about the servers on your network. If you wish to learn more about DNS and BIND, resources are listed at the end of this chapter.

BIND on Mac OS X Server

Mac OS X Server uses BIND version 8.2.3. You can start and stop DNS service on Mac OS X Server using the Server Settings application. You can use Server Status to view DNS status and usage statistics.

BIND Configuration File

By default, BIND looks for a configuration file labeled “named.conf” in the /etc directory. This file contains commands you can use to configure BIND’s many options. It also specifies the directory to use for zone data files.

Zone Data Files

Zone data files consist of paired address files and reverse lookup files. Address records link host names (host1.example.com) to IP addresses. Reverse lookup records do the opposite, linking IP addresses to host names. Address record files are named after your domain name—for example, db.example.com. Reverse lookup file names look like part of an IP address, such as db.192.168.12.

By default, the zone data files are located in
`/var/named/`

Practical Example

The following example allows you to create a basic DNS configuration using BIND for a typical network behind a Network Address Translation (NAT) device that connects to an ISP. The port (cable modem/DSL/dial-up/etc.) that is connected to your ISP is referred to here as the WAN port. The port that is connected to your internal network is referred to here as the LAN port. The sample files you need are installed with Mac OS X Server in the directories listed in the steps below. This example also assumes the following:

- The IP address of the WAN port is determined by your ISP.
- The IP address of the LAN port is 10.0.1.1
- The IP address of the Mac OS X or Mac OS X Server machine that will be used as the DNS server is 10.0.1.2.
- The IP addresses for client computers are 10.0.1.3 through 10.0.1.254.

If IP address assignment is provided by the NAT device via DHCP, it needs to be configured with the above information. Please consult your router or gateway manual for instructions on configuring its DHCP Server.

If your NAT device connects to the Internet, you also need to know the DNS server addresses provided by your ISP.

Setting Up Sample Configuration Files

The sample files can be found in:

`/usr/share/named/examples`

The sample files assume a domain name of example.com behind the NAT. This may be changed, but must be changed in *all* modified configuration files. This includes renaming `/var/named/db.example.com` to the given domain name, for example, `/var/named/db.foo.org`.

To set up the sample files:

- 1 Log in to the DNS server machine as root.
- 2 Choose Go To Folder from the Go menu.

- 3 In the “Go to the folder:” sheet, enter “/etc” (no quotation marks) and click the Go button.
- 4 Locate the file named.conf and rename it named.conf.OLD.
- 5 Launch the TextEdit application located in /Applications.
- 6 Copy the contents of /usr/share/named/examples/db.10.0.1.sample into a new file. Save the file as /var/named/db.10.0.1.
- 7 Copy the contents of /usr/share/named/examples/db.example.com.sample into a new file. Save the file as /var/named/db.example.com.
- 8 Copy the contents of /usr/share/named/examples/named.conf.sample into a new file.
- 9 Follow the instructions in the sample file to apply edits appropriate to your specific installation, then save the file as /etc/named.conf.
- 10 Log out and log back in as an administrator user.
- 11 Using Server Settings, via the Network tab, start the DNS service.
- 12 In the Network preference pane of System Preferences, change the domain name servers to list only the IP address of the new DNS server, 10.0.1.2.

Configuring Clients

If the IP addresses of your client computers are statically assigned, change the domain name servers of their Network preference panes to only list the new server’s IP address, 10.0.1.2.

If you are using Mac OS X Server as your DHCP Server:

- 1 In Server Settings, choose Configure DHCP from the Network tab.
- 2 On the Subnet tab, edit the built-in Ethernet port (default).
- 3 In the General tab, enter the following information:
Start: 10.0.1.3
End: 10.0.1.254
Subnet Mask: 255.255.255.0
Router: 10.0.1.1
- 4 Select the DNS tab and enter the following information:
Default Domain: example.com
DNS Servers: 10.0.1.2
- 5 Click the Save button and log out of Server Settings.

Note: The client computers may not immediately populate with the new IP configuration information. This will depend upon when their DHCP leases expire. It may be necessary to restart the client computers for the changes to populate.

Check Your Configuration

To verify the steps were successful, launch the Terminal application located in /Applications/Utilities and enter the following commands (substituting the local domain name for “example.com” if different):

```
nslookup server.example.com
nslookup 10.0.1.2
```

Note: If this generic configuration example does not meet your needs, Apple recommends that you do not attempt to configure DNS on your own and seek out a professional consultant or additional documentation.

Load Distribution With Round Robin

BIND allows for simple load distribution using an address shuffling method called *round robin*. You set up a pool of IP addresses for several hosts mirroring the same content, and BIND cycles the order of these addresses as it responds to queries. Round robin has no capability to monitor current server load or processing power. It simply cycles the order of an address list for a given host name.

You enable round robin by adding multiple address entries in your zone data file for a given host. For example, suppose you want to distribute Web server traffic between three servers on your network that all mirror the same content. Suppose the servers have the IP addresses 192.168.12.12, 192.168.12.13, and 192.168.12.14. You would add these lines to the zone data file db.example.com:

```
www.example.com 60 IN A 192.168.12.12
www.example.com 60 IN A 192.168.12.13
www.example.com 60 IN A 192.168.12.14
```

When BIND encounters multiple entries for one host, its default behavior is to answer queries by sending out this list in a cycled order. The first request gets the addresses in the order A, B, C. The next request gets the order B, C, A, then C, A, B, and so on. Notice that the TTL is set quite short to mitigate the effects of local caching.

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's unlikely that your local area network will ever 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, when you do connect to the Internet, 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.

Where to Find More Information

For more information on DNS and BIND, see the following:

- *DNS and BIND*, 4th edition, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 2001)
- The International Software Consortium Web site:
www.isc.org

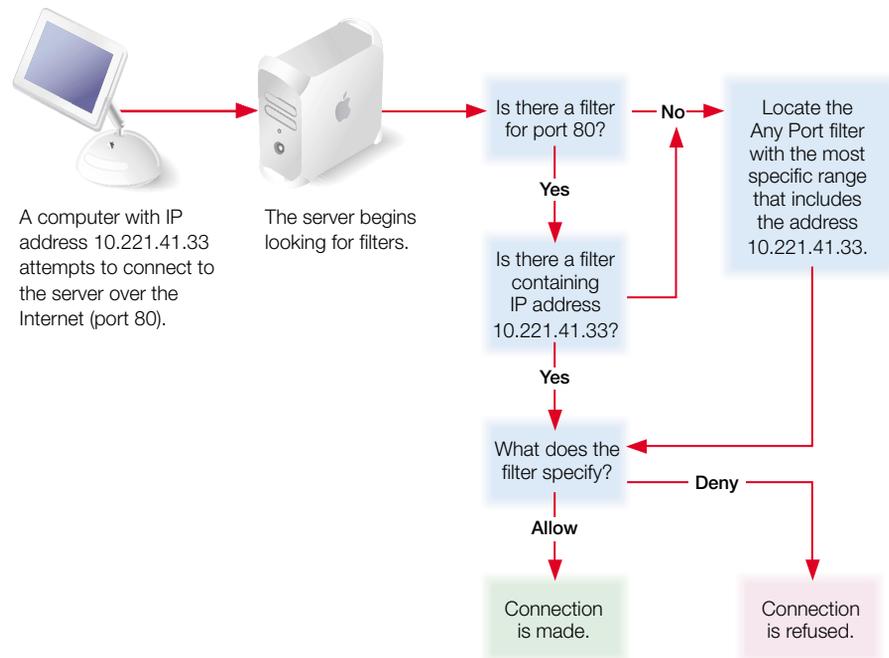
Firewall Service

Firewall service is software that protects the network applications running on your Mac OS X Server. Turning on Firewall service is similar to erecting a wall to limit access. Firewall 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 for a range of client IP addresses.

Services such as Web and FTP are identified on your server by a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number. When a computer tries to connect to a service, Firewall 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 picture 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 data.

Important When you start Firewall 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 Firewall service off, all addresses are allowed access to your server.

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 Firewall service. This service works well for small to medium businesses, schools, and small or home offices.

Large organizations with a firewall can use Firewall 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 Firewall service to control access to their own servers.

Mac OS X Server uses the ipfw software for firewall service.

Before You Set Up Firewall Service

When you start Firewall 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 Firewall 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 you can 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, and can be set to apply to all addresses.

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, and the last segment might belong 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 Settings, you enter an IP address and a subnet mask. Server Settings 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 following 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 the request 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 Firewall 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.

Practical Examples

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 Settings, 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

Setting Up Firewall Service for the First Time

Once you've decided which filters you need to create, follow these overview steps to set up Firewall service. If you need more help to perform any of these steps, see “Managing Firewall Service” on page 531 and the other topics referred to in the steps.

Step 1: Configure Firewall service

Configure Firewall service in Server Settings.

To configure Firewall service:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.

You can configure Firewall 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 “Managing Firewall Service” on page 531.

Step 2: Add filters to the IP filter list

Read “Before You Set Up Firewall Service” on page 527 to learn how IP filters work and how to create them.

To add IP filters:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Click New and create a filter.

For more information about creating a new filter, see “Creating an IP Filter” on page 532.

Step 3: Start Firewall service

- In Server Settings, click Firewall and choose Start Firewall.

Important If you add or change a filter after starting Firewall 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 Firewall service, computers already connected to your FTP server will be disconnected.

Managing Firewall Service

Check this section to find step-by-step instructions for setting up and configuring Firewall service.

Starting and Stopping Firewall Service

By default, Firewall service blocks all incoming TCP connections and allows all UDP connections. Before you turn on Firewall service, make sure you’ve set up filters allowing access from IP addresses you choose – otherwise, no one will have access to your server.

Important If you add or change a filter after turning on Firewall service, the new filter will affect connections already established with the server. For example, if you deny all access to your file server, computers already connected to your file server will be disconnected.

To start or stop Firewall service:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Start Firewall or Stop Firewall.

Setting Firewall Service to Start Automatically

If you plan to use Firewall service regularly, you should set the service to start automatically on startup. This ensures that your firewall is in place after a system restart or power outage.

To set Firewall service to start automatically each time your computer starts up:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Select “Start Firewall at system startup,” then click Save.

Editing IP Filters

If you edit a filter after turning on Firewall service, your changes affect connections already established with the server. For example, if any computers are connected to your Web server, and you change the filter to deny all access to the server, connected computers will be disconnected.

If you delete a port from the filter list, all IP filters for that port will also be deleted.

To edit IP filters:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Select a filter and click Duplicate, Edit, or Delete. If you are deleting a filter, you’ve finished.
- 4 Make any changes to the settings, then click Save.

Creating an IP Filter

IP filters contain an IP address and a subnet mask. You can apply a filter to all IP addresses, a specific IP address, or a range of IP addresses.

To create an IP filter:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Click New, or select a port or address that has a filter similar to the one you want to create, and click Duplicate.
- 4 Select whether this filter will allow or deny access.
- 5 Choose a port number from the pop-up menu, or enter the port number.

If you select a nonstandard port, you can enter a name that indicates the port’s use, such as Web or Apple file service.

- 6 Select the IP addresses that you want to filter.

If you choose a range of addresses, enter the beginning IP address for the range.

If you don’t know the IP address, click Find IP Address to search for an IP address. A search returns one IP address from the domain name you specified.

- 7 If you choose “a range of IP addresses,” enter a subnet mask or click Use My Subnet to use the computer’s subnet mask.

The resulting address range is displayed at the bottom of the window.

- 8 Click Save.

Searching for IP Filters

You can use the Find button in the IP Filter List window to search for filters that match specific criteria. For example, you may want to see what filters you have set up for a specific IP address.

To search the IP filter list:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Click the Find button.
- 4 Choose your search criteria from the pop-up menus.
- 5 Click Find.

The search results appear in the bottom half of the window.

Viewing the Firewall Log

Each filter you create in Server Settings corresponds to one or more “rules” in the underlying firewall software. Log entries show you the rule applied, the IP address of the client and server, and other information.

To view the log for Firewall service:

- 1 In Server Status, click your server in the Devices and Services list.
- 2 Click the Log tab and choose System Log.
- 3 Look for log entries with the prefix “ipfw.”

Configuring Firewall Service

By default, Firewall service blocks all incoming TCP connections and allows all UDP connections. Before you turn on Firewall service, make sure you’ve set up filters allowing access from IP addresses you choose; otherwise, no one will have access to your server.

Important If you add or change a filter after turning on IP filtering, the new filter will affect connections already established with the server. For example, if you deny all access to your file server, computers already connected to your file server will be disconnected.

To configure Firewall service:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Select “Start Firewall at system startup” if you want the service to start whenever the server starts up.
- 4 Select “Send rejection to client if connection is denied” if you want your server to respond to denied connection attempts (this is on by default).
- 5 Choose which connections (allowed or denied) you want to log.
- 6 Click the NetInfo and Advanced tabs if you want to make configuration settings for UDP, ICMP, IGMP, and NetInfo.
- 7 Click Save, then restart Firewall service.

Setting Up Logs for Firewall Service

You can log only the packets that are denied by the filters you set, only the packets that are allowed, or both. Both logging options can generate a lot of log entries, which can fill up disk space and degrade the performance of the server. You should use “Log all allowed packets” only for limited periods of time.

To set up logs:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Select the logging options you want, then click Save.
- 4 Restart Firewall service.

Server Status provides access to all of Mac OS X Server’s service logs. Click your server in the Devices and Services list, then choose System Log and look for entries that begin with “ipfw.”

The filters you create in Server Settings 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 538.

Here are some examples of firewall 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 Firewall 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 Firewall 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 Firewall service used rule 10 to send a packet to itself on port 660 via the loopback device 0.

Viewing Denied Packets

Viewing denied packets can help you identify problems and troubleshoot Firewall service.

To view denied packets:

- 1 Turn on logging of denied packets in the Configure Firewall window.
- 2 To view log entries in Server Status, click your server in the Devices and Services list.
- 3 Click the Log tab and choose System Log from the pop-up menu.

Filtering UDP Ports in Firewall Service

Many services use User Datagram Protocol (UDP) to communicate with the server. By default, all UDP connections are allowed. You should apply filters to UDP ports sparingly, if at all, because “deny” filters could create severe congestion in your server traffic.

If you filter UDP ports, don't select the “Log all allowed packets” option in the General pane. Since UDP is a “connectionless” protocol, every packet to a UDP port will be logged if you select that option.

You should also create allow filters for specific services, including

- 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
- NetInfo

UDP ports above 1023 are allocated dynamically by certain services, so their exact port numbers may not be determined in advance.

To set up UDP port filters:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Click the Advanced tab and select “Apply filters in IP filter list to UDP ports.”
- 4 Click “all UDP ports” or enter a range of port numbers to filter in the “in range” fields.
- 5 Click Save, then restart Firewall service.

Blocking Multicast Services in Firewall Service

Some hosts and routers use Internet Gateway Multicast Protocol (IGMP) to send packets to lists of hosts. Keep in mind that denying IGMP packets may prevent services that use multicast addressing from running correctly. QuickTime Streaming uses multicast addressing, as does Service Location Protocol (SLP).

To block IGMP connections:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Click the Advanced tab and select Deny Internet Gateway Multicast Protocol (IGMP).
- 4 Click Save, then restart Firewall service.

Allowing NetInfo Access to Certain IP Addresses

Any information stored in a shared NetInfo domain needs to be accessed by multiple Mac OS X computers on the network. You can use Firewall service to control which IP addresses can access a particular shared domain.

To allow NetInfo access:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Click the NetInfo tab and select a shared domain from the “Network visible domain” pop-up menu.
- 4 Choose “everyone” to allow all IP addresses to access the domain.

To restrict access to certain IP addresses, enter IP addresses in the text field, pressing Return between entries.

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.

- 5 Click Save, then restart Firewall service.

Any IP filters you create allow NetInfo access for the IP addresses you specify. By default, NetInfo dynamically chooses a TCP or UDP port from the 600 through 1023 range, but you can configure a shared domain to be accessible using one port or using a port for TCP and a second port for UDP packets.

If you choose to allow access to all IP addresses, you should have a firewall that protects your internal network from the Internet and blocks external traffic targeted at the ports used for NetInfo. If you don't have a separate firewall, selecting all IP addresses could compromise your server's security.

Changing the Any Port (Default) Filter

If the server receives a packet using a port or IP address to which none of your filters apply, Firewall service uses the Any Port (default) filter. You can set the Any Port (default) filter to either deny or allow these packets for specific IP addresses. By default the Any Port filter denies access.

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.

To change the default Any Port setting:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Show Firewall List.
- 3 Select Any Port and click New, or select an IP address under Any Port and click Edit.
- 4 Make any changes to the settings, then click Save.

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 IP address and force the server to keep replying, locking out others who are trying to connect to the server. This is one type of denial-of-service attack.

To prevent denial-of-service attacks:

- 1 In Server Settings, click the Network tab.
- 2 Click Firewall and choose Configure Firewall.
- 3 Make sure "Send rejection to client if connection is denied" is not checked.
- 4 Click the Advanced tab and select "Deny ICMP echo (ping) reply."

- 5 Click Save, then restart Firewall service.

Important Denial-of-service attacks are somewhat rare, so make these settings only if you think your server may be vulnerable to an attack. If you don't send rejection replies to clients, some clients may retry connections, resulting in server congestion. Also, if you deny ICMP echo replies, services that use pinging to locate network services will be unable to detect your server.

Creating IP Filter Rules Using ipfw

You can use the ipfw command in conjunction with the Firewall module of Server Settings when you want to

- Display rules created by the Firewall module. Each filter translates into one or more rules.
- Create filters with characteristics that cannot be defined using the Firewall 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 Firewall module. Changes you make to Firewall module rules are not permanent. Firewall service recreates any rules defined using the Firewall module whenever the service is restarted. Here is a summary of how the Firewall module assigns rule numbers:

Rule number	Used by Firewall 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 Firewall window.
63300	Denying access for igmp. Created when Deny IGMP is selected in the Advanced pane of the Configure Firewall 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.

Rule number	Used by Firewall module for
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 Firewall window to allow all or specific clients to access those ports.
64000–65000	User-defined filters for Any Port.

Reviewing IP Filter Rules

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

When you type:

```
ipfw show
```

You see information similar to this:

```
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
...
```

Creating IP Filter Rules

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
```

Deleting IP Filter Rules

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.

Port Reference

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)	
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
137	Windows Names	
138	Windows Browser	
139	Windows file and print (SMB)	RFC 100
143	IMAP (email access)	RFC 2060

TCP port	Used for	Reference
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)	
625	Remote Directory Access	
626	IMAP Administration (Mac OS X mail service and AppleShare IP 6.x mail)	
636	LDAP SSL	
660	Server Settings	
985	NetInfo (when a shared domain is created using NetInfo Domain Setup)	
1220	QTSS Admin	
1694	IP Failover	
1723	PPTP VPN	
2049	NFS	
3283	Apple Remote Desktop	
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)	
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)	

Solving Problems

This section reviews some common Firewall service issues and provides possible solutions.

You Can't Access the Server Over TCP/IP

- Check the filters in the filter list. If you started Firewall service, but have not added any additional filters, all TCP access to your server is denied by default.
- Stop Firewall service. Add new filters to your filter list that allow access to computers that have the IP addresses you specify. Then restart Firewall service.

You Can't Locate a Specific Filter

- Use the Find button in the IP Filter List window to locate specific filters by IP address, port, or access type.

Where to Find More Information

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 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

- 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.

SLP DA Service

Service Location Protocol Directory Agent (SLP DA) 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 the service manually. When a client computer needs to locate a network service, it uses SLP to look for that type of service. 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.

SLP DA Considerations

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 Begin

Before you set up SLP DA service, read these overview steps to learn about defining scopes and making sure of client and router compatibility.

Step 1: Define 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.

Step 2: Check 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. When tunneling is set up, the router passes along IP multicast packets. See the documentation that came with your routers for information on tunneling.

Step 3: 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 “Managing Service Location Protocol (SLP) Directory Agent (DA) Service” on page 547.

Step 4: Create scopes for your network

When you start SLP service, one scope already exists, named Default. You can change that name or add more scopes to your network.

To create scopes:

- 1** In Server Settings, click the Network tab.
- 2** Click SLP Service and choose Show Registered Services.
The Registered Services window appears.
- 3** Click New Scope and type the name of the scope you are creating in the Add Scope dialog box.

SLP DA service converts the name you type to the correct format and adds it to the list in the Registered Services window.

Step 5: Assign network services to each scope

Once you've created a scope, you can assign network services to it.

- 1 In the Registered Services window, click New Service.
- 2 In the Add Proxied Service dialog box, choose the scope and add the service you want.

For more information about adding services to a scope, see “Registering a Service With SLP DA” on page 548.

Step 6: Start SLP DA service

To start SLP DA service:

- 1 Click SLP Service.
- 2 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.

Managing Service Location Protocol (SLP) Directory Agent (DA) Service

This section describes day-to-day management tasks for SLP DA service.

Starting and Stopping SLP DA Service

Use Server Settings to start and stop SLP DA service.

To start or stop SLP DA service:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Start SLP DA or Stop SLP DA.

When the service is running, a globe appears on the SLP icon. It may take a moment for the service to start (or stop).

Viewing Scopes and Registered Services in SLP

You can view scopes and the services registered within the scopes in the Registered Services window of SLP DA service. This window also shows the name, IP address and service type for each service in the list.

To view scopes and registered services:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Show Registered Services.

- 3 Choose a service type from the Show pop-up menu.
- 4 Click the disclosure triangle next to a scope name to see the services registered within it.
- 5 Double-click a service to see more detailed information about the service.

You can change the way the list is sorted by clicking a column heading.

Creating New Scopes in SLP DA Service

Scopes are groups of services available on the network, organized in a way that works best for your network.

To create a new scope and add services to it:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Show Registered Services.
- 3 Click New Scope.
- 4 Type a name for the scope and click OK.
- 5 Click New Service.
- 6 Choose the scope you just created from the pop-up menu, then type the URL of the service you're adding in the URL field.
- 7 Click OK.

You can also enter information about the service in the Attribute List field. If you enter attributes, they must be in the correct format, or SLP DA service may not recognize the service.

Registering a Service With SLP DA

You can register services available on the network with SLP DA to make them easily discoverable by client users.

To register a service:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Show Registered Services.
- 3 Click New Service and choose a scope from the pop-up menu.
- 4 Type the URL of the service you're adding in the URL field.
- 5 If you want to use an attributes list, type the attributes in the Attribute List text box.
- 6 Click OK.

Important If you enter information about the service in the Attribute List field, make sure the attributes are in the correct format or SLP DA may not recognize the service.

Deregistering Services in SLP DA Service

If a service is no longer available to network clients you must manually remove the service from the SLP DA registered service list.

To deregister a service:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Show Registered Services.
- 3 Select a service and click Remove.

Setting Up Logs for SLP DA Service

SLP DA errors are logged automatically in the system log file. You can choose other events to log when you configure SLP DA service.

To set SLP DA logging options:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service and choose Configure SLP DA.
- 3 Select the types of events you want to log and click Save.

Logging Debugging Messages in SLP DA Service

In addition to the basic logging options available in the Configure SLP window, you can choose to log all messages, including debugging messages. These messages are useful to advanced system administrators.

To log debugging messages:

- 1 In Server Settings, click the Network tab.
- 2 Click SLP Service.
- 3 Hold down the Option key and choose Configure SLP DA.
- 4 Click All Messages and click Save.

Viewing SLP DA Log Entries

You can view the system log for SLP event messages.

To view log entries for SLP DA service:

- 1 In Server Status, click the Log tab.
- 2 Choose System Log from the pop-up menu and look for entries in the log that include "slpd:".

Each SLP log entry includes a code that indicates the type of event that has occurred.

Code	Event type
REG	Service registrations and deregistrations
EXP	Service deregistrations only
SR	Service requests
DA	Directory agent information requests
ERR	SLP errors

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
```

The directory agent must scan any included attributes lists 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.

Where to Find More Information

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 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 SLP DA, see RFC 2608.

Tools for Advanced Users

This chapter describes tools, and techniques intended for use by experienced server administrators. The following table summarizes them.

Tool or technique	Use to	For more information, see
Terminal	Run command-line tools	page 552
Secure shell (SSH)	Use Terminal to run command-line tools for remote servers	page 553
dsimportexport	Import and export user and group accounts using XML or text files	page 555
log rolling scripts	Periodically roll, compress, and delete server log files	page 555
diskspacemonitor	Monitor percentage-full disk thresholds and execute scripts that generate email alerts and reclaim disk space when thresholds are reached	page 556
diskutil	Manage Mac OS X Server disks and volumes remotely	page 557
installer	Install software packages remotely	page 558
softwareupdate	Find new versions of software and install them remotely on a server	page 561
systemsetup	Configure system preferences on a remote server	page 561
networksetup	Configure network services for a particular network hardware port on a remote server	page 562

Tool or technique	Use to	For more information, see
MySQL Manager	Manage the version of MySQL that is installed with Mac OS X Server	page 565
Simple Network Management Protocol (SNMP) administration tools	Monitor your server using the SNMP interface	page 566
diskKeyFinder	Verify the physical location of a remote headless server volume that you want to manage	page 566
Enabling IP failover	Set up a standby server that takes over if the primary server fails	page 567

Terminal

You use the Terminal application to run command-line tools. Most of the tools described in this chapter are command-line tools, such as `dsimportexport`, `systemsetup`, `networksetup`, and `diskutil`.

Using the Terminal Application

Terminal lets you open a UNIX shell command-line session on your server or a remote server you are administering. You'll find Terminal in `/Applications/Utilities/`.

When you open Terminal, you see a prompt that usually includes the name of the local host, the directory you're using, your user name, and a symbol (for example, "[patsy6:/usr/sbin] liz%"). In this example, `patsy6` is the server's host name, the directory you are working in is `/usr/sbin`, and the user name is `liz`.

The percent symbol (%) is called the *prompt*. It indicates that you can enter a command. Press the Return key after you type a command. Depending on what you typed, you could see a list of information followed by another prompt, or your command will execute and give you some type of feedback and a prompt, or you will receive no feedback and another prompt. No feedback usually means that the command was executed properly.

Understanding UNIX Command-Line Structure

UNIX commands share some basic conventions. First you enter the name of the tool, then any information the tool needs to carry out your request. Most tools come with help or man (short for “manual”) pages that describe how to use the tool. Help pages give an overview of *arguments* (also known as *options* or *parameters*) that the tool understands. Man pages give more detail and examples:

- To find help pages, type the name of the tool and then the argument “-help” (for example, “dsimportexport -help”).
- To find man pages for a tool, type “man”, followed by the tool name (for example, “man ssh”).

When you supply information in a command, enclose location or item names that include spaces in quotation marks (“like this”).

Secure Shell (SSH) Command

Secure Shell (SSH) lets you send secure, encrypted commands over a network. With SSH turned on, you can use the Terminal application to open an SSH session and use command-line tools to securely configure a remote server. You can also connect a terminal to a headless server through the serial port and log in using SSH.

For complete information about SSH, type “man ssh” in Terminal.

Enabling and Disabling SSH Access

Access to Mac OS X computers using SSH is enabled by default.

You can disable SSH access to a Mac OS X computer locally or remotely:

- When logged in locally to a Mac OS X computer, make sure that “Remote login” in the Sharing pane is not selected.
- To disable SSH access to a remote server, while in an SSH session with the remote computer, type “systemsetup -setremotelogin off”.

You can reenable SSH access only locally.

Opening an SSH Session

Open an SSH session and log into a remote server when you manage the remote server using command-line tools.

To open an SSH session and log in to the server:

- 1 Open Terminal.

- 2 At the prompt, type `ssh`, then a hyphen, the flag “l” (lower case L, for “login”) followed by the user name of an administrator of the remote server and the server’s IP address or host name. Press Return when you’re finished (for example, “`ssh -l jsmith 192.168.100.100`”).

If you’re not sure of the administrator’s name, you can also type “`ssh admin@192.168.100.100`”.

If you don’t enter an administrator name (or “admin”), SSH will use the user name of the person currently logged in to the computer you are using. If this user doesn’t have administrator access to the server, you must enter the appropriate administrator name.

- 3 At the prompt, type the administrator password and press Return.

If everything is entered correctly, the prompt identifies the remote server (for example, `[192.168.100.100:~] jsmith%`).

If you started the remote server up from a CD and logged in as root, you will see a number sign (#) instead of the remote server identifier.

Executing Commands in an SSH Session

Once you are logged in using SSH, you can use command-line tools to execute commands on the remote server.

If you want to execute a single command on the server and then immediately log out of the server, you can do it in one step. Type your login information and the command, then press Return.

For example, the command to log in to a remote server and remove a file called “Test Data” looks like this: “`ssh -l root 192.168.100.100 rm "/Documents/Test Data"`”. The server asks for the password, and then executes the command.

Closing an SSH Session

When you have finished with a SSH session, you should close the session, especially if you are logged in as the root administrator with root privileges, so that no one else can make changes on the server. To log out, simply type “exit”, then press Return.

Understanding Key Fingerprints

The first time you log in to a server using SSH, your local computer adds a “fingerprint” from the remote server to a list of known remote host computers and displays a message:

The authenticity of host ‘192.168.12.12’ can’t be established.

RSA key fingerprint is a8:0d:27:63:74:00:f1:04:bd:6a:e4:0d:a3:47:a8:f7.

Are you sure you want to continue connecting (yes/no)?

Enter “yes” and press Return to finish authenticating.

If you see a warning message about a “man in the middle attack” when you try to connect using SSH, the RSA key fingerprint on the remote server and the computer you are using to administer it no longer match. This can happen if you use command-line tools to administer a remote server, establish an RSA key fingerprint, and later change your SSH configuration, perform a clean install of system software, or start up from the Mac OS X Server CD.

To connect to the remote server again using SSH, you need to edit the entries corresponding to the hosts (which can be stored by both name and IP number) in this file: `~/ssh/known_hosts`. You can use TextEdit or another editor to find the host name or IP address and then delete the key. The key is a long string that may wrap to several lines. In TextEdit you can press the Control key and type K to delete the line, and then delete the blank line that the deletion creates.

dsimportexport

Use `dsimportexport` to import user and group accounts from a file or export them to a file. It is a useful tool when you want to

- Create a large number of users or groups in a batch.
- Migrate user or group accounts from another server. You can import users and groups from AppleShare IP 6.3 or Mac OS X Server version 10.1 and earlier.
- Update a large number of user or group accounts with new information.

See “Importing and Exporting User and Group Information” on page 178 for more information about `dsimportexport`.

Log Rolling Scripts

Three predefined scripts are executed automatically to reclaim space used on your server for log files generated by

- Apple file service
- Windows service
- Web service
- Web performance cache
- Mail service
- Print service

The scripts use values in predefined configuration files to determine whether and how to reclaim space:

- The script `/etc/periodic/daily/600.daily.server` runs daily. Its configuration file is `/etc/diskspacemonitor/daily.server.conf`.

- The script `/etc/periodic/weekly/600.weekly.server` is intended to run weekly, but is currently empty. Its configuration file is `/etc/diskspacemonitor/weekly.server.conf`.
- The script `/etc/periodic/monthly/600.monthly.server` is intended to run monthly, but is currently empty. Its configuration file is `/etc/diskspacemonitor/monthly.server.conf`.

As configured, the scripts specify actions that complement the log file management performed by the services listed above, so do not modify them. All you need to do is log in as an administrator and use a text editor to define thresholds in the configuration files that determine when the actions are taken:

- the number of megabytes a log file must contain before its space is reclaimed
- the number of days since a log file's last modification that need to pass before its space is reclaimed

Specify one or both thresholds. The actions are taken when either threshold is exceeded.

There are several additional parameters you can specify. Refer to comments in the configuration files for information about all the parameters and how to set them. The scripts ignore all log files except those for which at least one threshold is present in the configuration file.

To configure the scripts on a server from a remote Mac OS X computer, open a Terminal window and log in to the remote server using `ssh`. Then open a text editor and edit the scripts.

You can also use the `diskspacemonitor` command-line tool to reclaim disk space.

diskspacemonitor

When you need more vigilant monitoring of disk space than the log rolling scripts provide, you can use the `diskspacemonitor` command-line tool. It lets you monitor disk space and take action more frequently than once a day when disk space is critically low, and gives you the opportunity to provide your own action scripts.

`diskspace monitor` is disabled by default. You can enable `diskspacemonitor` by opening a Terminal window and typing `sudo diskspacemonitor on`. You may be prompted for your password. Type `man diskspacemonitor` for more information about the command-line options.

When enabled, `diskspacemonitor` uses information in a configuration file to determine when to execute alert and recovery scripts for reclaiming disk space:

- The configuration file is `/etc/diskspacemonitor/diskspacemonitor.conf`. It lets you specify how often you want to monitor disk space and thresholds to use for determining when to take the actions in the scripts. By default, disks are checked every 10 minutes, an alert script executed when disks are 75% full, and a recovery script executed when disks are 85% full. To edit the configuration file, log in to the server as an administrator and use a text editor to open the file. See the comments in the file for additional information.

- By default, two predefined action scripts are executed when the thresholds are reached. The default alert script is `/etc/diskspacemonitor/action/alert`. It runs in accord with instructions in configuration file `/etc/diskspacemonitor/alert.conf`. It sends email to recipients you specify.
The default recovery script is `/etc/diskspacemonitor/action/recover`. It runs in accord with instructions in configuration file `/etc/diskspacemonitor/recover.conf`.
See the comments in the script and configuration files for more information about these files.
- If you want to provide your own alert and recovery scripts, you can. Put your alert script in `/etc/diskspacemonitor/action/alert.local` and your recovery script in `/etc/diskspacemonitor/action/recovery.local`. Your scripts will be executed before the default scripts when the thresholds are reached.

To configure the scripts on a server from a remote Mac OS X computer, open a Terminal window and log in to the remote server using SSH.

diskutil

This Mac OS X tool is especially useful in a server environment, because it offers a wide variety of commands for managing and repairing disks. For example:

- To list the disks and partitions on the Mac OS X computer you are logged into, type “`diskutil list`” in a Terminal window.
- To create a Redundant Array of Independent Disks (RAID) set on multiple disks, type “`sudo diskutil createRAID mirror MirrorDisk BootableHFS+ disk1 disk2`”. Root access is required.
- To verify the disk structure of a volume, type “`sudo diskutil verifyDisk /Volumes/SomeDisk`”. To repair the disk structure, type “`sudo diskutil repairDisk /Volumes/SomeDisk`”. Root access is required.
- To verify permissions of a Mac OS X boot volume, type “`sudo diskutil verifyPermissions /`”. Root access is required.

Type “`man diskutil`” in a Terminal window for complete information about this command.

To run `diskutil` on a Mac OS X computer from a remote Mac OS X computer, open a Terminal window and log in to the remote computer using SSH.

installer

You can use the installer tool to install software packages from a CD-ROM on a mounted remote server volume. This tool doesn't perform any authentication, so if a package needs authentication (set in the package's .info file), you must log in as root or use the sudo command.

Remember that copyright laws may prevent certain programs from being shared. Before putting programs inside shared folders, check the applicable licensing agreements and follow their requirements.

Using installer

Here are the parameters that installer accepts. Parameters are delimited using angle brackets (<>) if they are required and square brackets ([]) if they are optional:

```
installer [-volinfo] [-pkginfo] [-allow] [-dumplog]
          [-help] [-verbose] [-vers] [-config] [-plist]
          [-file pathToFile] [-lang isoLanguageCode]
          <-pkg pathToPackage> <-target pathToDestinationVolume>
```

where

-volinfo

displays a list of mounted volumes into which the software package can be installed.

-pkginfo

displays a list of packages that can be installed onto the target volume. If a metapackage is specified, all of its subpackages are listed.

-allow

installs an older version over a newer version if the software package supports this.

-dumplog

sends the standard installer log to StdOut.

-help

displays a list of parameters you can use with the installer tool.

-verbose

displays more information than the default output, which is formatted for scripting. Use this parameter in conjunction with information requests.

-vers

displays the version of the tool.

-config

formats the command-line installation arguments for later use. You can redirect the output to a configuration file. Then you can use the `-file` parameter to perform multiple identical installs.

-plist

formats the installer tool's output into an XML file, which is sent by default to StdOut. You use this parameter with `-pkginfo` and `-volinfo`.

-file pathToFile

specifies the path to an XML file containing parameter information. This file can be used instead of the command-line parameters and supersedes any parameters on the command-line (for example, "installer -file /temp/configfile.plist").

-lang isoLanguageCode

specifies the default language of the installed system. You need this parameter only if you perform a full system install. You specify the language in ISO language code format: EN for English, JA for Japanese, FR for French, and DE for German.

-pkg pathToPackage

specifies where to find the package you want to install. Don't end the pathname string with a forward slash (/) or the command will not execute.

-target pathToDestinationVolume

specifies where to install the package. Don't end the pathname string with a forward slash (/) or the command will not execute.

To use installer to install software on a server:

- 1 Insert the application disk in the optical drive of the remote server on which you want to install the software.
- 2 Open an SSH connection in Terminal and log in to the remote server.
- 3 Type an installer command.
- 4 If the software package you're installing requires that you restart the server, type `"/sbin/reboot"` or `"/sbin/shutdown -r"`.

Full Operating System Installation

If you have to install the operating system on a remote Mac OS X Server, you can use the installer tool to do so.

To use installer to install a full operating system:

- 1 Insert a bootable CD and start up the server from the CD. (You can't install an operating system onto the current startup volume.)

- 2 Open Terminal on another Mac OS X Server or administrator computer and log in to the server as root using SSH. For example, type:

```
ssh -l root <ip address>
```

- 3 Mount volumes using the autodiskmount tool. To do this, type:

```
autodiskmount
```

Important Don't use the disk utility and installer applications after you use autodiskmount to manually mount volumes until *after* you have restarted your server. Otherwise, you will get unreliable results.

- 4 List the volumes available to install the software on and specify the package you want to install. For example, type:

```
/usr/sbin/installer -volinfo -pkg /System/Installation/Packages/  
OSInstall.mpkg
```

and get a list. The information displayed reflects your particular environment, but here's an example:

```
/private/var/tmp/Mount01  
/private/var/tmp/Mount1  
/private/var/tmp/Mount02
```

- 5 Install the operating system on a volume from the list. For example, to use Mount01 in the example in step 4, type:

```
/usr/sbin/installer -pkg /System/Installation/Packages/OSInstall.mpkg  
-target /private/var/tmp/Mount01 -lang en -verbose
```

to get this result:

```
installer: Package name is Mac OS X  
installer: Installing onto volume mounted at  
/private/var/tmp/Mount01.  
installer: The install was successful.
```

- 6 Type one of these commands to restart the server:

```
/sbin/reboot  
/sbin/shutdown -r
```

Important Apple strongly recommends that you not store data on the hard disk or hard disk partition where the operating system is installed. With this approach, you will not risk losing data should you need to reinstall or upgrade system software.

softwareupdate

You use `softwareupdate` to find new versions of software and install them on a remote server.

To use softwareupdate:

- 1 Open Terminal on a Mac OS X Server or administrator computer and log in to the remote server using SSH.
- 2 At the prompt, type “`softwareupdate`”. Available updates are listed.
- 3 Type “`softwareupdate`” followed by the items you want to install (for example, “`softwareupdate PrintingEpsonUS Printing EpsonEU`”). The tool downloads and installs the software on the remote server.
- 4 If the new software requires you to restart the remote server, type “`/sbin/reboot`” or “`/sbin/shutdown -r`”.

systemsetup

You use `systemsetup` to remotely configure these system preferences: sleep settings; remote login (SSH); startup disk; computer name; and date, time, and time-zone settings.

To use `systemsetup`, open Terminal on a server or administrator computer and open an SSH session on the remote server whose preferences you want to set up. Type one of the following commands to review complete information about `systemsetup`:

- “`systemsetup -printcommands`” displays all the available commands.
- “`systemsetup -help`” displays commands plus explanations of them.
- “`man systemsetup`” displays the most complete information, including examples.

You use “`get`” options to retrieve settings and “`set`” options to change them:

- “`systemsetup -getusingnetworktime`” may display “Network Time: Off”.
- “`systemsetup -setusingnetworktime on`” starts a network time server.

Working With Server Identity and Startup

You can use `systemsetup` to set information about a remote server and specify how to handle its startup:

- To set the computer name, which is used by file sharing and AppleTalk, type “`systemsetup -setcomputername <computer name>`”.
- To retrieve the current startup disk for the server, type “`systemsetup -getstartupdisk`”.
Type “`systemsetup -liststartupdisks`” to list all available disks.
Type “`systemsetup -setstartupdisk <disk name>`” to set the startup disk, specifying the disk name exactly as formatted in the list.

- Type “systemsetup -setrestartpowerfailure on” to restart the server automatically after a power failure.
- To restart the server automatically if it freezes, type “systemsetup -setrestartfreeze on”.
- To enable the server to respond to events sent by other computers, such as AppleScript programs, type “systemsetup -setremoteappleevents on”.

Working With Date and Time Preferences

You can use systemsetup to set up date and time preferences for a remote server:

- To set the current month, day, and year, type “systemsetup -setdate <mm:dd:yy>”.
- To set the current hour, minutes, and seconds, type “systemsetup -settime <hh:mm:ss>”.
- To set the server’s time zone, type “systemsetup -settimezone <timezone>”. To determine which timezone values are valid, type “systemsetup -listtimezones”.
- To designate a network time server, type “systemsetup -setnetworktimeserver <ip address or dns name>”.
- To turn network time on, type “systemsetup -setusingnetworktime on”.

Working With Sleep Preferences

You can use systemsetup to set when a remote server sleeps and whether the server wakes for different types of network activity. Remember, however, that while a server is asleep, you can’t administer it remotely:

- To specify how many minutes the server can be inactive before going to sleep, type “systemsetup -setsleep <minutes>”. If you don’t want the server to sleep, type “0” or “never”.
- To specify that the server should wake from sleep when modem activity is detected, type “systemsetup -setwakeonmodemactivity on”.
- To specify that the server should wake from sleep when a network admin packet is sent to it, type “systemsetup -setwakeonnetworkaccess on”.

networksetup

Use networksetup to configure network services on a remote Mac OS X Server. A *network service* is a complete collection of settings for a specific network hardware port. “Built-in Ethernet” is an example of a network service.

You may have one or several network services for a given hardware port. With networksetup you can

- enable or disable network services

- create new network services
- set the order of network services
- configure the TCP/IP options of the network services
- set other networking options for the services, such as proxy server information

To use `networksetup`, open Terminal on a server or administrator computer and open an SSH session on the remote server whose preferences you want to set up. Type one of the following commands to review complete information about `networksetup`:

- “`networksetup -printcommands`” displays all the available commands.
- “`networksetup -help`” displays commands plus explanations of them.
- “`man networksetup`” displays the most complete information, including examples.

Reverting to Previous Network Settings

When you change your network preference settings with `networksetup`, your previous settings are saved to the `com.apple.preferences.xml.old` file located in

`/var/db/SystemConfiguration/com.apple.preferences.xml.old`

Note that if you make changes to network settings locally using Network preferences, the settings in the `com.apple.preferences.xml.old` file will not match the settings you make using `networksetup`.

If you want to revert to your previous settings, rename the file “`com.apple.preferences.xml`” and then restart the server.

If network settings prevent you from accessing a server using SSH, log in to the server locally as root and rename the file “`com.apple.preferences.xml`” (replacing the current file). Restart the server to apply the settings.

Retrieving Your Server’s Network Configuration

You can use `networksetup` to find out about the network services on a remote server:

- To display a list of network services in the order in which they are contacted for a connection along with the corresponding ports and devices, type “`networksetup -listnetworkserviceorder`”. An asterisk (*) next to a service means the service is inactive.
- To display a list of all network services, type “`networksetup -listallnetworkservices`”. An asterisk (*) next to a service means the service is inactive.
- To display a list of hardware ports with corresponding device names and Ethernet addresses, type “`networksetup -listallhardwareports`”.
- To detect new hardware and create a default network service on the hardware, type “`networksetup -detectnewhardware`”.
- To display the IP address, subnet mask, router, and Ethernet address for a particular network service, type “`networksetup -getinfo <network service>`”.

Configuring TCP/IP Settings

You can use `networksetup` to configure TCP/IP settings:

- To specify a manual configuration for a network service, type “`networksetup -setmanual <network service> <ip address> <subnet mask> <router>`”.
- To set the TCP/IP configuration for a specified network service to use DHCP, type “`networksetup -setdhcp <network service> [client id]`”.
- To specify an address to use for DHCP, type “`networksetup -setmanualwithdhcprouter <network service> <ip address>`”.
- To set the TCP/IP configuration for the specified network service to use BOOTP, type “`networksetup -setbootp <network service>`”.

Configuring DNS Servers and Search Domains

You can use `networksetup` to specify how you want network services to use Domain Name System (DNS):

- To specify the IP addresses of servers you want a network service to use to resolve domain names, type “`networksetup -setdnsservers <network service> <dns server1> [dns server2] [...]`”. To clear all entries for the network service, type “empty” in place of a DNS server name.
- Type “`networksetup -setsearchdomains <network service> <domain1> [domain2] [...]`” to designate the search domain for the network service. To clear all search domain entries for the network service, type “empty” in place of the domain name.

Managing Network Services

You can use `networksetup` to create or rename network services, turn them on or off, remove them, and change the order in which they’re contacted. This application is also useful for displaying the names of hardware ports:

- To display all hardware port names, type “`networksetup -listallhardwareports`”.
- To create a new network service on a port, type “`networksetup -createnetworkservice <new network service> <hardware port>`”.
- To duplicate an existing network service, type “`networksetup -duplicatenetworkservice <network service> <new network service name>`”.
- To rename a network service, type “`networksetup -renamenetworkservice <network service> <new network service name>`”.
- To delete a network service, type “`networksetup -removenetworkservice <network service>`”. If there is only one network service for a port, you can’t delete it using this option. Instead, use `-setnetworkserviceenabled` to turn a network service off.
- To turn a network service on, type “`networksetup -setnetworkserviceenabled <network service> on`”.

- To turn AppleTalk on, type “networksetup -setappletalk <network service> on”.
- To turn passive FTP on, type “networksetup -setpassiveftp <network service> on”.
- To set the order in which network services are contacted on a particular port, type “networksetup -ordernetworkservices <service1> <service2> [...]”.

Designating Proxy Servers

You can use networksetup to designate servers to be used as proxies for some services:

- To set up proxy servers, use these networksetup commands:
 - setftp proxy <network service> <domain> <port number>
 - setweb proxy <network service> <domain> <port number>
 - setsecureweb proxy <network service> <domain> <port number>
 - setstreaming proxy <network service> <domain> <port number>
 - setgopher proxy <network service> <domain> <port number>
 - setsocksfirewall proxy <network service> <domain> <port number>
- To enable or disable the proxy settings, use these networksetup commands:
 - setftp proxy state <network service> <on or off>
 - setweb proxy state <network service> <on or off>
 - setsecureweb proxy state <network service> <on or off>
 - setstreaming proxy state <network service> <on or off>
 - setgopher proxy state <network service> <on or off>
 - setsocksfirewall proxy state <network service> <on or off>
- To designate bypass domains that you want to use for a network service, type “networksetup -setproxybypassdomains <network service> <domain1> <domain2> [...]”. To clear all bypass domain entries for the network service, type “empty” in place of a domain name.

MySQL Manager

You use MySQL Manager to manage the version of MySQL that is installed with Mac OS X Server. MySQL provides a relational database management system for hosting information you want to make available and manage using a Web site.

It lets you

- initialize the MySQL database
- start the MySQL process and make sure it starts automatically when the server restarts
- shut down the MySQL process and keep it from starting when the server restarts

You’ll find MySQL Manager in /Applications/Utilities/MySQL Manager.app.

Simple Network Management Protocol (SNMP) Tools

SNMP is a set of standard protocols used to manage and monitor multiplatform computer network devices.

SNMP uses agents to contact network devices such as routers and servers. SNMP interacts with these devices using virtual databases known as management information bases (MIBs). Vendors provide MIBs that describe their devices so that they can be monitored using SNMP applications.

Mac OS X Server comes with a MIB that lets you use SNMP tools to view a server's system and network usage statistics. To use SNMP on your server, use a graphical browser (not supplied with your server) or the SNMP command-line tool available in `/usr/sbin`.

SNMP support in Mac OS X Server is turned off by default. To turn it on, use TextEdit or another application to edit the `/etc/hostconfig` file on the server. If you turn SNMP on, you should run the `snmpconf` command to enter site-specific information, such as system location and admin email address. Type “`man snmpconf`” in a Terminal window to learn about `snmpconf`.

You can find SNMP information and tools on the Net-SNMP Home Page, located at www.net-snmp.com

diskKeyFinder

You can use the `diskKeyFinder` tool to verify the physical location of a remote headless server volume that you want to manage. When you specify the `bsd` file system name for a volume using `diskKeyFinder`, you'll see the drive bay where the volume is located (for example, Bay 2).

To find the `bsd` file system name of a volume, log in to the server using SSH and type “`df -l`”.

The output from this command shows the `bsd` file name and volume path. For example:

Filesystem	Mounted On
<code>/dev/disk0s13</code>	<code>/</code>
<code>/dev/disk0s9</code>	<code>/Volumes/Spare3</code>
<code>/dev/disk0s10</code>	<code>/Volumes/Holding</code>
<code>/dev/disk0s11</code>	<code>/Volumes/Spare1</code>
<code>/dev/disk0s12</code>	<code>/Volumes/Spare2</code>

In this example, `disk0` has five partitions (also known as slices) named 9, 10, 11, 12, and 13. If you want to know the physical location of partition 10, type “`/System/Library/ServerSetup/diskKeyFinder /dev/disk0s10`”.

The tool returns the drive bay number where the volume is located. Headless server drive bays are numbered in ascending order from left to right.

Enabling IP Failover

IP failover allows a secondary server to acquire the IP address of a primary server if the primary server ceases to function. Once the primary server returns to normal operation, the secondary server relinquishes the IP address. This allows your Web site to remain available on the network even if the primary server is temporarily offline.

Note: IP failover only allows a secondary server to acquire a primary server's IP address. You need additional software tools such as `rsync` to provide capabilities such as mirroring the primary server's data on the secondary server. See `rsync`'s man pages for more information.

Requirements

IP failover is not a complete solution, rather one tool you can use to increase your server's availability to your clients. In order to use IP failover you will need to set up the following hardware and software.

Hardware

IP failover requires the following hardware setup:

- primary server
- secondary server
- public network (servers must be on same subnet)
- private network between the servers (additional network interface card)

See "Setting Up a Private TCP/IP Network" on page 523 for more information on private networks.

Note: Because IP failover uses broadcast messages, both servers must have IP addresses on the same subnet of the *public* network. In addition, both servers must have IP addresses on the same subnet of the *private* network.

Software

IP failover requires the following software setup:

- unique IP addresses for each network interface (public and private)
- software to mirror primary server data to secondary server
- scripts to control failover behavior on secondary server (optional)

Failover Operation

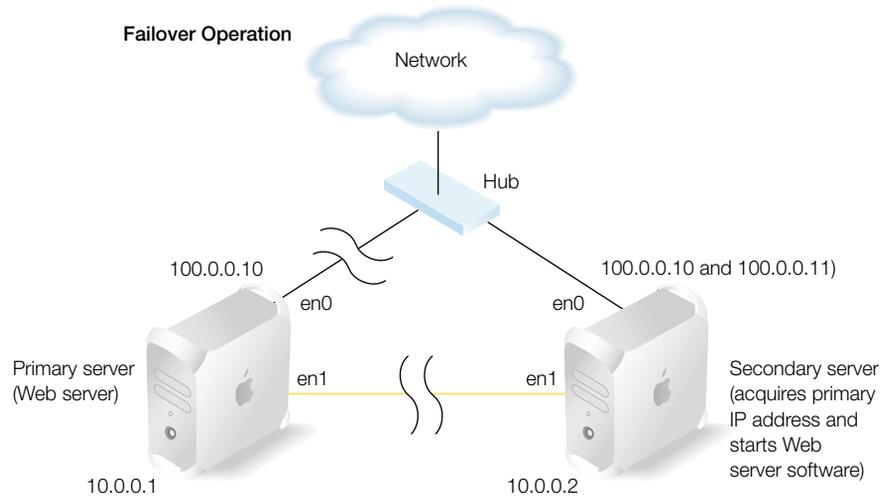
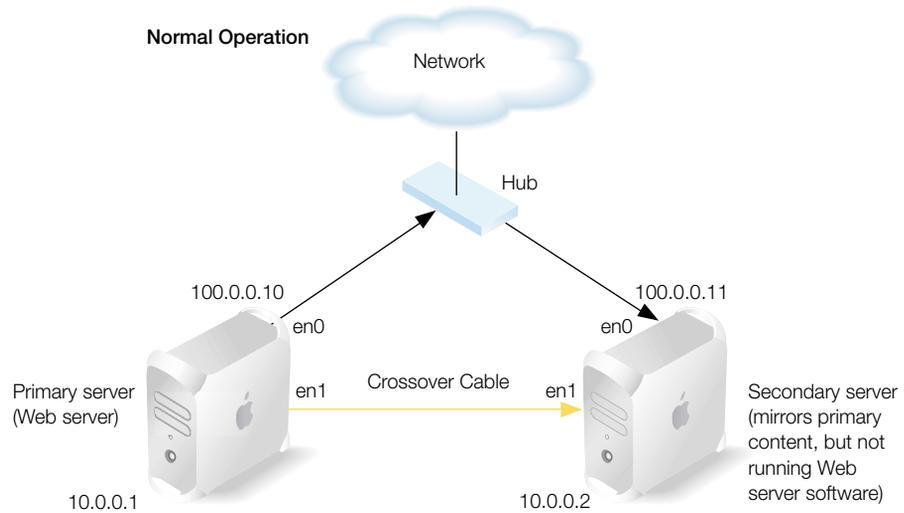
When IP failover is active, the primary server periodically broadcasts a brief message confirming normal operation on both the public and private networks. This message is monitored by the secondary server.

- If the broadcast is interrupted on both public and private networks, the secondary server initiates the failover process.

- If status messages are interrupted on only one network, the secondary server sends email notification of a network anomaly, but does not acquire the primary server's IP address.

Email notification is sent when the secondary server detects a failover condition, a network anomaly, and when the IP address is relinquished back to the primary server.

Normal operation and failover operation are illustrated in the following two diagrams.



Enabling IP Failover

You enable IP failover by adding command lines to the file `/etc/hostconfig` on the primary and the secondary server. Be sure to enter these lines exactly as shown with regard to spaces and punctuation marks.

To enable IP failover:

- 1 At the primary server, add the following line to `/etc/hostconfig`:

```
FAILOVER_BCAST_IPS="10.0.0.255 100.0.255.255"
```

Substitute the broadcast addresses used on your server for the public and private networks. This tells the server to send broadcast messages over relevant network interfaces that the server at those IP addresses is functioning.

- 2 Restart the primary server so that your changes can take effect.
- 3 At the secondary server, add the following lines to `/etc/hostconfig`:

```
FAILOVER_PEER_IP="10.0.0.1"  
FAILOVER_PEER_IP_PAIRS="en0:100.0.0.10"  
FAILOVER_EMAIL_RECIPIENT="admin@example.com"
```

In the first line substitute the IP address of the primary server on the private network.

In the second line enter the local network interface that should adopt the primary server's public IP address, a colon, then the primary server's public IP address.

(Optional) In the third line, enter the email address for notification messages regarding the primary server status. If this line is omitted, email notifications are sent to the root account on the local machine.

- 4 Restart the secondary server so that your changes can take effect.

Important Always be sure that the primary server is up and functioning normally before you activate IP failover on the secondary server. If the primary server is not sending broadcast messages, the secondary server will initiate the failover process and acquire the primary's public IP address.

Configuring IP Failover

You configure failover behavior using scripts. The scripts must be executable (for example, shell scripts, Perl, compiled C code, or executable AppleScripts). You place these scripts in a directory named "IPFailover" in the Library directory of the secondary server. Check the IPFailover directory for sample scripts.

You need to create a directory named with the public IP address of the primary server to contain the failover scripts for that server. For example:

```
/Library/IPFailover/100.0.0.10
```

Notification Only

You can use a script named “Test” located in the failover scripts directory to control whether, in the event of a failover condition, the secondary server acquires the primary’s IP address, or simply sends an email notification. If no script exists, or if the script returns a zero result, then the secondary server acquires the primary’s IP address. If the script returns a non-zero result, then the secondary server skips IP address acquisition and only sends email notification of the failover condition. The test script is run to determine whether the IP address should be acquired and to determine if the IP address should be relinquished when the primary server returns to service.

A simple way to set up this notification-only mode is to copy the script located at `/usr/bin/false` to the directory named with your primary server IP address and then change the name of the script to “Test”. This script always returns a non-zero result.

Using the Test script, you can configure the primary server to monitor the secondary server, and send email notification if the secondary server becomes unavailable.

Pre And Post Scripts

You can configure the failover process with scripts that can run before acquiring the primary IP address (preacquisition), after acquiring the IP address (postacquisition), before relinquishing the primary IP address (prerelinquish) and after relinquishing the IP address back to the primary server (postrelinquish). These scripts reside in the `/Library/IPFailover/<IP address>` directory on the secondary server, as previously discussed. The scripts use these four prefixes:

- PreAcq—run before acquiring IP address from primary server
- PostAcq—run after acquiring IP address from primary server
- PreRel—run before relinquishing IP address back to primary server
- PostRel—run after relinquishing IP address back to primary server

You may have more than one script at each stage. The scripts in each prefix group are run in the order their file names would appear in a directory listing using the `ls` command.

For example, your secondary server may perform other services on the network such as running a statistical analysis application and distributed image processing software. A preacquisition script quits the running applications to free up the CPU for the Web server. A postacquisition script starts the Web server. Once the primary is up and running again, a prerelinquish script quits the Web server, and a postrelinquish script starts the image processing and statistical analysis applications. The sequence of scripted events might look like this:

```
<Failover condition detected>
Test (if present)
PreAcq10.StopDIP
```

```
PreAcq20.StopSA
PreAcq30.CleanupTmp
<Acquire IP address>

PostAcq10.StartTimer
PostAcq20.StartApache

<Primary server returns to service>

PreRel10.StopApache
PreRel20.StopTimer

<Relinquish IP address>
PostRel10.StartSA
PostRel20.StartDIP
PostRel30.MailTimerResultsToAdmin
```


Open Directory Data Requirements

This appendix contains tables that specify the data requirements of Open Directory domains. Use the information in the following tables when mapping Mac OS X data types to attributes in LDAP or Active Directory domains:

- User Data That Mac OS X Server Uses (p. 573)
- Standard Data Types in User Records (p. 574)
- Format of the MailAttribute Data Type (p. 577)
- Standard Data Types in Group Records (p. 580)

User Data That Mac OS X Server Uses

The following table describes how your Mac OS X Server uses data from user records in directory domains. Consult this table to determine the data items that your server's various services need to retrieve from directory domains. Note that "All services" in the far-left column include AFP, SMB, FTP, HTTP, NFS, WebDAV, POP, IMAP, Workgroup Manager, Server Settings, Server Status, 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)

Server component	Data item used	Dependency
All services	PrimaryGroupID	Optional, but recommended. Used for authorization (for example, file permissions and mail accounts).
FTP service	HomeDirectory	Optional
Web service	NFSHomeDirectory	
Apple file service		
NFS service		
Macintosh Manager		
Mac OS X login window		
Application and system preferences		
Mail service	MailAttribute	Required for login to mail service on your server
Mail service	EEmailAddress	Optional

Standard Data Types in User Records

The following table specifies the standard data types found in Open Directory user records.

Important When mapping attributes of a read/write directory domain (a domain that is not read-only), do not map the distinguished name and the first short name to the same data type. If these attributes are mapped to the same data type, serious problems will occur when you try to edit the distinguished name in Workgroup Manager.

Data type	Format	Sample values
RecordName: a list of names associated with a user; all attributes used for authentication must map to this data type	ASCII characters A-Z, a-z, 0-9, _, -, .	Dave David Mac DMacSmith Non-zero length, at least one instance. Maximum 255 characters (127 double-byte characters) per instance, 16 instances per record.
RealName: a single name, usually the user's full name; not used for authentication	ASCII	David L. MacSmith, Jr. Non-zero length, maximum 255 characters (127 double-byte characters).

Data type	Format	Sample values
UniqueID: a unique user identifier, used for access privilege management	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. Normally unique among entire population of users, but sometimes can be duplicated. Warning: A non-integer value is interpreted as 0, which is the UniqueID of the root user.
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 1 to 4,294,967,295. Normally unique among entire population of group records.
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 (this value prevents users with accounts in the directory domain from accessing the server remotely via a command line) Non-zero length.
AuthenticationHint: text set by the user to be displayed as a password reminder	ASCII	Your guess is as good as mine. Maximum 255 bytes.
NFSHomeDirectory: local file system path to the user's home directory	ASCII	/Network/Servers/example/Users/K-M/Tom King Non-zero length. Maximum 255 bytes.
Picture: file path to a recognized graphic file to be used as a display picture for the user	ASCII	Maximum 255 bytes.

Data type	Format	Sample values
MCXSettings: stores preferences for a managed user	Mac OS X property list	
AuthenticationAuthority: an XML description of the user's defined method for authentication.	ASCII	Values are used to describe SASL server authentication, Kerberos authentication, directory-based authentication, or crypt and replacement crypt authentication. Absence of this data type signifies legacy authentication/password management.
MailAttribute: a user's mail service configuration (refer to "Format of the MailAttribute Data Type" on page 577 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>

Data type	Format	Sample values
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	user@example.com mailto:user@example.com
HomeDirectory: the location of an AFP-based home directory	Mac OS X property list	<p><homeDir> <url>afp://server/sharepoint</url> <path>usershomedirectory</path> </homeDir></p> <p>In the following example, Tom King's home directory is K-M/Tom King, which resides beneath the share point directory, Users:</p> <p><homeDir> <url>afp://example.com/Users</url> <path>K-M/Tom King</path> </homeDir></p>

Format of the MailAttribute Data Type

Ensure that each MailAttribute data type you configure your server to retrieve from an LDAP or Active Directory 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	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>

MailAttribute field	Format	Sample values
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>
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>

MailAttribute field	Format	Sample values
NotificationStaticIPValue	<p>An optional IP address, in bracketed, dotted decimal format ([xxx.xxx.xxx.xxx]).</p> <p>If this field is missing, NotificationState is interpreted as "NotificationLastIP."</p> <p>The field is used only when NotificationState has the value "NotificationStaticIP."</p>	<pre><key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string></pre>
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>

Standard Data Types in Group Records

The following table specifies the standard data types found in Open Directory group records.

Data type	Format	Sample values
RecordName: name associated with a group	ASCII characters A-Z, a-z, 0-9, _, -, .	Science Science_Dept Science.Teachers Non-zero length, maximum 255 characters (127 double-byte characters).
RealName: usually the group's full name	ASCII	Science Department Teachers Non-zero length, maximum 255 characters (127 double-byte characters).
PrimaryGroupID: a user's primary group association	Unsigned 32-bit ASCII string of digits 0–9	Range is 0 to 4,294,967,295. Normally unique among entire population of group records.
GroupMembership: a list of short names of user records that are considered part of the group	ASCII characters A-Z, a-z, 0-9, _, -, .	bsmith, jdoe Can be an empty list (normally for users primary group).
HomeDirectory: the location of an AFP-based home directory for the group	Mac OS X property list	<homeDir > <url >afp://server/sharepoint</url > <path >grouphomedirectory</path > </homeDir > In the following example, the Science group's home directory is K-M/Science, which resides beneath the share point directory, Groups: <homeDir > <url >afp://example.com/Groups</url > <path >K-M/Science</path > </homeDir >
MCXSettings: stores preferences for a workgroup (a managed group)	Mac OS X property list	



Glossary

This glossary defines terms and spells out abbreviations you may encounter while working with online help or the “Mac OS X Server Administrator’s Guide.” References to terms defined elsewhere in the glossary appear in *italics*.

A, B

administrator A user with server or *directory domain* administration privileges. Administrators are always members of the predefined “admin” group.

administrator computer A Mac OS X computer onto which you have installed the server applications from the Mac OS X Server Admin CD.

AFP (Apple Filing Protocol) A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses *TCP/IP* and other protocols to communicate between computers on a network.

authentication authority attribute A value that identifies the password validation scheme specified for a user and provides additional information as required.

BIND (Berkeley Internet Name Domain) The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or *named*, when the program is running.

boot ROM Low-level instructions used by a computer in the first stages of starting up.

BSD (Berkeley System Distribution) A version of UNIX on which Mac OS X software is based.

C

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

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.

child A computer that gets configuration information from the shared directory domain of a *parent*.

computer account A list of computers that have the same preference settings and are available to the same users and groups.

D, E

DHCP (Dynamic Host Configuration Protocol) A protocol used to distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then 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.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a *directory node* or simply a directory.

directory domain hierarchy A way of organizing local and shared directory domains. A hierarchy has an inverted tree structure, with a root domain at the top and local domains at the bottom.

directory node See *directory domain*.

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

disk image A file that when opened (using Disk Copy) creates an icon on a Mac OS desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software.

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

drop box A shared folder with privileges that allow other users to write to, but not read, the folder's contents. Only the *owner* has full access. Drop boxes should only be created using AFP. When a folder is shared using AFP, the ownership of an item written to the folder is automatically transferred to the owner of the folder, thus giving the owner of a drop box full access to and control over items put into it.

dynamic IP address An IP address that is assigned for a limited period of time or until the client computer no longer needs the IP address.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a Web site visitor.

export The Network File System (NFS) term for sharing.

F, G

filter A “screening” method used to control access to your server. 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.

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

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.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group directory A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among them.

guest computer An unknown computer that is not included in a computer account on your server.

guest user A user who can log in to your server without a user name or password.

H

home directory A folder for a user’s personal use. Mac OS X also uses the home directory, for example, to store system preferences and managed user settings for MacOS X users.

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 linking and 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 ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

idle user A user who is connected to the server but hasn't used the server volume for a period of time.

IGMP (Internet Group Management Protocol) An Internet protocol used by hosts and routers to send packets to lists of hosts that want to participate, in a process known as *multicasting*. QuickTime Streaming Server (QTSS) 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 remains on the server until the user deletes it.

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

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 domain.

lease period A limited period of time during which IP addresses are assigned. By using short leases, DHCP can reassign IP addresses on networks that have more computers than available IP addresses.

load balancing The process of distributing the demands by client computers for network services across multiple servers in order to optimize performance by fully utilizing the capacity of all available servers.

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

local home directory A home directory for a user whose account resides in a local NetInfo or LDAPv3 directory domain.

long name See *user name*.

LPR (Line Printer Remote) A standard protocol for printing over TCP/IP.

M

mail host The computer that provides your mail service.

managed client A user, group, or computer whose access privileges and/or preferences are under administrative control.

managed preferences System or application preferences that are under administrative control. Server Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients. Macintosh Manager allows administrators to control both system preferences and application preferences for Mac OS 9 and Mac OS 8 managed clients.

MBONE (multicast backbone) A virtual network that supports IP multicasting. An MBONE network uses the same physical media as the Internet, but is designed to repackage multicast data packets so they appear to be unicast data packets.

MIBS (management information bases) Virtual databases that allow various devices to be monitored using SNMP applications.

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. You determine how you want the server to respond when it receives files with certain suffixes. Each suffix and its associated response make up a MIME type mapping.

MTA (mail transfer agent) A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

multihoming The ability to support multiple network connections. When more than one connection is available, Mac OS X selects the best connection according to the order specified in Network preferences.

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

N

name server See *DNS (Domain Name System)*.

NetBIOS (Network Basic Input/Output System) A program that allows applications on different computers to communicate within a local area network.

NetBoot server A Mac OS X server on which you have installed NetBoot software and have configured to allow clients to start up from disk images on the server.

NetInfo The Apple protocol for accessing a directory domain.

Network File System (NFS) 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.

network installation The process of installing systems and software on Mac OS X client computers over the network. Software installation can occur with an administrator attending the installations or completely unattended.

nfsd daemon An *NFS* server process that runs continuously behind the scenes and processes reading and writing requests from clients. The more daemons that are available, the more concurrent clients can be served.

NSL (Network Service Locator) The Apple technology that simplifies the search for TCP/IP-based network resources.

O

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use *LDAP*, *NetInfo*, or *Active Directory* protocols; *BSD* configuration files; and network services.

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

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

owner The person who created a file or folder and who therefore has the ability to assign access privileges for other users. The owner of an item automatically has read and write privileges for an item. An owner can also transfer ownership of an item to another user.

P, Q

parent A computer whose shared directory domain provides configuration information to another computer.

percent symbol (%) The command-line prompt in the Terminal application. The prompt indicates that you can enter a command.

PHP (PHP: Hypertext Preprocessor) A scripting language embedded in HTML that is used to create dynamic Web pages.

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

predefined accounts User accounts that are created automatically when you install Mac OS X. Some group accounts are also predefined.

preferences cache A storage place for computer preferences and preferences for groups associated with that computer. Cached preferences help you manage local user accounts on portable computers.

presets Initial default attributes you specify for new accounts you create using Server Manager. You can use presets only during account creation.

primary group A user's default group. The file system uses the ID of the primary group when a user accesses a file he or she doesn't own.

primary group ID A unique number that identifies a primary group.

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

proxy server A server that sits between a client application, such as a Web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

QTSS (QuickTime Streaming Server) A technology that lets you deliver media over the Internet in real time.

R

realm See *WebDAV realm*.

relay point See *open relay*.

Rendezvous A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks.

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.

S

scope A group of services. 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.

SDP (Session Description Protocol) A file used with QuickTime Streaming Server that provides information about the format, timing, and authorship of a live streaming broadcast.

search path See *search policy*.

search policy A list of directory domains searched by a Mac OS X computer when it needs configuration information; also the order in which domains are searched. Sometimes called a search path.

shadow image A file, hidden from regular system and application software, used by NetBoot to write system-related information while a client computer is running off a server-based system disk image.

share point A folder, hard disk (or hard disk partition), or CD that is accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using *AFP*, Windows *SMB*, *NFS* (an “export”), or *FTP* protocols.

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

Simplified Finder A user environment featuring panels and large icons that provide novice users with an easy-to-navigate interface. Mounted volumes or media to which users are allowed access appear on panels instead of on the standard desktop.

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, the service uses SLP to register itself on the network. SLP/DA uses 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 protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SNMP (Simple Network Management Protocol) A set of standard protocols used to manage and monitor multiplatform computer network devices.

spam Unsolicited email; junk mail.

SSL (Secure Sockets Layer) An Internet protocol that allows you to send encrypted, authenticated information across the Internet.

static IP address An IP address that is assigned to a computer or device once and is never changed.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration.

System-less clients Computers that do not have operating systems installed on their local hard disks. System-less computers can start up from a disk image on a NetBoot server.

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. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

Tomcat The official reference implementation for Java Servlet 2.2 and JavaServer Pages 1.1, two complementary technologies developed under the Java Community Process.

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.

UID (user ID) A number that uniquely identifies a user. Mac OS X computers use the UID to keep track of a user’s directory and file ownership.

Unicode A standard that assigns a unique number to every character, regardless of language or the operating system used to display the language.

URL (Uniform Resource Locator) The address of a computer, file, or resource that can be accessed on a local network or 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.

user name The long name for a user, sometimes referred to as the user’s “real” name. See also *short name*.

V

virtual user An alternate email address (short name) for a user.

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, and then check them back in while a site is running.

WebDAV realm A region of a Website, usually a folder or directory, that is defined to provide access for WebDAV users and groups.

wildcard A range of possible values for any segment of an IP address.

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.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

X, Y, Z



Index

A

- access logs 227
- access privileges
 - about 124, 205
 - administrator 206
 - copying 217
 - directory services and 71
 - everyone 207
 - explicit vs. inherited 206, 207
 - group 206
 - guests 210
 - guest users 129
 - hierarchy 207
 - managing share points 217
 - of administrators 125
 - owner 206
 - restricting 222
 - role of group ID 125
 - role of UID in 124, 125
 - security guidelines 222
 - setting for WebDAV 339
 - setting in AppleShare client software 219
 - setting in Windows 219
 - setting share points 211
 - user categories 206
 - Web sites 340, 342
- accounts
 - Guest Computers 277
 - managing preferences, Mac OS X 282
- Active Directory
 - ADSI (Active Directory Services Interface) 104
 - configuring 104–105
 - creating server configuration 104
 - directory service protocol 74
 - Open Directory support 104
 - populating domains with data 105
 - search policies and 105
 - adding users to groups 148
 - admin group 125, 129, 131
 - administration
 - planning 92
 - remote 58
 - administrative data
 - how used by server 573
 - mapping 573–580
 - administrative data. *See* directory domains
 - administrator
 - access privileges 206
 - access to mail database 394
 - choosing for directory services 92
 - defined 581
 - modifying account 137
 - passwords 137
 - administrator accounts
 - backing up 202
 - administrator computer
 - defined 58, 581
 - administrator privileges
 - directory domain 126, 145
 - local computer 126
 - server 145
 - server administration 125
- AFP
 - defined 581
 - home directories in 165

- AFP (Apple Filing Protocol) 224
- AirPort base stations
 - DHCP service and 477
- All Other Computers account 429, 452
- All Other Users account 429, 430
- anonymous FTP 249
- Anonymous FTP User predefined account 130
- Apache 365
- Apache modules 365–367
- Apache Web server
 - configuration 338
 - resources 64
- APOP (Authenticated POP) 384
- Apple Fileing Protocol (AFP)
 - setting up sharing 212
- Apple file server 530
- Apple file service
 - access log 232
 - Access settings 226
 - allowing guest access 234
 - archiving logs 233
 - automatically disconnecting idle users 234
 - automounting share point in Mac OS X 260
 - automounting share point on Mac OS 8 or 9
 - client 261
 - changing language 418
 - changing server name 231
 - configuring 225
 - connecting to server in Mac OS 8 and 9 261
 - connecting to server in Mac OS X 259
 - described 221
 - enabling AppleTalk browsing 232
 - features 224
 - General settings 225
 - Idle Users settings 228
 - limiting connections 232
 - Logging settings 227
 - login greeting 234
 - Mac OS 8 and 9 client software
 - requirements 260
 - Mac OS X client software requirements 259
 - monitoring 229
 - planning 225
 - problems with 263
 - registering with NSL 231
 - sending users messages 235
 - solving problems 263
 - specifications 224
 - starting 229
 - starting automatically 231
 - stopping 230
 - viewing logs 230
- Apple file services
 - See also* Apple Filing Protocol (AFP)
- Apple Filing Protocol (AFP)
 - defined 581
 - home directories in 160
 - key features of 49
 - Macintosh Manager 446
 - resharing NFS mounts in 215
- AppleShare 263
- AppleShare IP 6.3
 - AFP compared to 224
- AppleTalk 224, 226, 263
 - enabling and disabling for Open Directory 93
 - file service protocol 72
- attributes, directory domain
 - about 71
 - adding 102
 - mapping LDAPv3 101
- attributes list 550
- authentication
 - Apple file service 224
 - directory data and 70
 - FTP service 254
 - Kerberos 224, 248, 254
 - mail service 381, 384, 385, 389
 - NFS service 222
 - Password Server 88
 - planning 91
 - protocols supported 88
 - search policy 94
 - solving problems 203
 - Windows services 236
- authentication authority attribute 192
 - defined 581
- Authentication Manager 237, 264
 - backing up 119
- automatic search policy
 - See also* search policies

- about 83
- adding Active Directory server to 105
- adding LDAPv2 server to 107
- adding LDAPv3 server to 99, 100
- LDAPv3 mappings supplied by 103
- using 95
- automounting
 - directory services and 71
 - share points 207
- available directory domains
 - listing accounts in 174

B

- backing up
 - directory services 119
 - Password Server 201
 - root and administrator user accounts 202
- BCC 382
- Berkeley Internet Name Domain (BIND)
 - defined 581
- Berkeley System Distribution (BSD)
 - defined 581
- .bin (MacBinary) format 247
- bin (predefined group account) 131
- BIND 515, 516, 518, 520–523
 - about 520
 - configuration File 520
 - configuring 520–523
 - defined 520, 581
 - example 521–523
 - load distribution 523
 - zone data files 521
- binding
 - configuring NetInfo 111
 - kinds of NetInfo 111
 - machine records for 113
- black-hole servers 375
- blind carbon copies 382
- BootP protocol 476
- boot ROM
 - defined 581
- Boot Server Discovery Protocol (BSDP) 491
- broadcast binding, configuring Netinfo 112
- BSD
 - defined 581

- BSD configuration files
 - DSFFPlugin.plist file for 115
 - enabling and disabling 93
 - history of 67
 - mapping data 115
 - Open Directory and 74, 115
 - populating with data 118
- bsdpd_client 493

C

- CA certificate 361
- cache. *See* proxy cache
- canonical name
 - defined 581
- capacity planning
 - NetBoot 488
- certificate file 361–363
- CGI
 - defined 582
- CGI programs
 - problems with 364
- CGI scripts
 - enabling 354–355
 - installing 354
 - solving problems 364
- child computer
 - defined 582
- child NetInfo domain 110
- Chooser
 - setting up printing via AppleTalk 324
- Classic
 - installing on Mac OS X disk image 497
- client computers
 - customizing 45, 52
 - encoding for older clients 226
 - installing software over the network 509
 - SLP DA service 546
 - startup up using N key 507
 - system requirements 488
- client computers (Mac OS 8 and 9)
 - using Apple file service 260
- client computers (Mac OS X)
 - using Apple file service 259
- client computers (Windows)
 - using file services 261

- using Windows services 262
- client computers, Mac OS 8 and 9
 - setting up printing 324
- client computers, Mac OS 9
 - selecting NetBoot startup image 506
- client computers, Mac OS X
 - selecting NetBoot startup image 506
 - setting up printing 323
- client computers, UNIX
 - print service 325
- client computers, Windows
 - print service 325
- client management, Mac OS 9 and 8 411
 - See also* Macintosh Manager
 - about 411
 - access privileges 440
 - administrator computer requirements 415
 - application settings 457
 - benefits of 414
 - client computer requirements 414
 - copying Mac OS 8 preferences 464
 - guest access 429
 - making items available to users 438, 440
 - Managed Preferences folder 466
 - managing portable computers 461
 - media access 465
 - more information 473
 - mounting volumes 446
 - planning 414
 - printing 448
 - setting access privileges 442
 - setting login options 460
 - setting up administration computer 416
 - setting up computer lists 451
 - setting up Mac OS 9 client computers 416, 417
 - setting up printing 447
 - setting up workgroups 436, 438
 - setup overview 424
 - sharing information 443, 444
 - solving problems 470, 471, 472
 - transition strategies 412
 - upgrading 412
 - user experience 412
 - using NetBoot 423
 - using update package 417
- client management, Mac OS X
 - See also* Workgroup Manager 267
 - about 267
 - administrator computer requirements 269
 - administrators 270
 - benefits of 269
 - client computer requirements 269
 - computer accounts 271, 272
 - group accounts 271
 - guest computers 277
 - managing preferences 282
 - planning 269
 - presets 273
 - transition strategies 268
 - user accounts 270
 - user experience 268
- code page 238
- command-line tools. *See* Terminal
- Common Gateway Interface (CGI)
 - defined 582
- compressed files 247
- computer accounts
 - about 128
 - adding to 274
 - changing information 274
 - creating 272
 - defined 582
 - deleting 276
 - deleting computers from 275
 - Guest Computer 277
 - moving computers between 275
 - presets 273
 - searching for 276
- computer accounts, Mac OS 9 and 8. *See* Macintosh Manager
- computer list, Mac OS 9 and 8 425
- computer list, Mac OS X. *See* computer accounts
- computer lists, Mac OS 9 and 8
 - See also* Macintosh Manager
- computer preferences
 - managing, Mac OS X 286
- computers, Mac OS X
 - controlling access to 278
- configuration files. *See* BSD configuration files

- Configure Web Service window 342
- CRAM-MD5 385, 389
- cross-platform issues for file service 236
- CSR (certificate signing request) 361–362
- custom FTP root 253
- custom root in FTP 248

D

- daemon (predefined group account) 131
- database
 - directory domain 66
 - mail service 373
 - Password Server 88
- data types
 - group records 580
 - MailAttribute 577–579
 - user records 574–577
- Desktop Printer Utility
 - setting up LPR printing 324
- DHCP
 - about 54
 - defined 582
- DHCP servers 476
 - interactions 477
 - network location 476
- DHCP service 475–484
 - AirPort base stations 477
 - automatic search policy and 84
 - deleting subnets 480
 - described 475
 - DNS options for subnets 482
 - DNS Server for DHCP Clients 479
 - LDAP auto-configuration 477
 - LDAP server for DHCP clients 479
 - logs 480, 483
 - logs for 478
 - managing 478–484
 - managing subnets 481–483
 - monitoring clients 481
 - more information 484
 - NetInfo binding 112
 - NetInfo options for subnets 482
 - planning 475–477
 - preparing for setup 475–477
 - setting up 477–478

- solving Problems 484
- starting 478
- stopping 478
- subnet IP addresses lease times,
 - changing 480
- subnets 476
 - subnets, creating 481
 - uses for 475
 - viewing client lists 483
- dialer (predefined group account) 131
- Directory Access application 59
 - Active Directory server, adding 104
 - automatic search policy, using 95
 - BSD configuration files, mapping 116
 - custom search policies, defining 96
 - enabling and disabling protocols 94
 - LDAPv2 106–110
 - LDAPv2 access, changing 107
 - LDAPv2 configuration, adding 106
 - LDAPv2 search bases and data mapping,
 - editing 108
 - LDAPv3 97–103
 - LDAPv3 access via DHCP 97
 - LDAPv3 configuration, adding 98
 - LDAPv3 configuration, changing 99
 - LDAPv3 configuration, deleting 100
 - LDAPv3 configuration, duplicating 99
 - LDAPv3 configurations, showing and hiding 97
 - LDAPv3 connections, changing 100
 - LDAPv3 search bases and mappings,
 - editing 101
 - local domain search policy 96
 - NetInfo binding, configuring 112
 - remote administration 118
 - search policies 94–96
- Directory Agent (DA) 547
- directory domain
 - defined 582
 - user accounts in 122
- directory domain hierarchies
 - about 78–84
 - data visibility in 81, 86
 - examples 79–80, 81
 - NetInfo 110, 111

- planning 82, 85–87, 91
 - search policies for 82–84
- directory domain hierarchy
 - defined 582
- directory domains
 - See also* BSD configuration files, LDAPv2, LDAPv3, local directory domains, NetInfo, shared directory domains
 - about 73
 - administrative data in 86
 - defined 45
 - information storage in 66, 71
 - limiting users in 91
 - mail service configuration in 376
 - security 87
 - simplifying changes to 86
 - tools for managing 89
 - user accounts in 66–67
- directory node
 - defined 582
- directory services
 - See also* Open Directory
 - about 47
 - administrators for 92
 - authentication 67
 - backing up 119
 - benefits of 65
 - defined 45, 582
 - information storage in 65
 - logs 119
 - network role of 66
 - planning 90, 91
 - setup overview 90
 - status 119
 - tools summary 89
- disconnect messages 229
- disk images 485, 492
- disk images, Network Install
 - creating 511
 - enabling 514
- diskKeyFinder 566
- disk space
 - monitoring 555
 - reclaiming logs' use of 555
- diskspacemonitor 556
- diskutil 557
- DNS (Domain Name System)
 - defined 582
 - Rendezvous 72
- DNS server
 - default for DHCP 479
- DNS servers 516
- DNS service 515–524
 - A records 396
 - configuring BIND 520–523
 - described 515
 - junk mail prevention with 375, 399
 - load distribution 523
 - mail service and 372, 377
 - managing 518–520
 - more information 524
 - MX records 372, 377, 381, 396
 - planning 516–517
 - preparing for setup 516
 - problems with 264
 - reverse lookups 396
 - setting up 517
 - setup overview 517–518
 - starting 518, 519
 - stopping 518
 - strategies 516–517
 - usage statistics 519
 - uses for 515
 - with mail service 516
- Documents folder 341
- domain browsing services 240
- domain names
 - registering 517
- Domain Name System (DNS)
 - about 54
 - defined 582
- DoS (Denial of Service) attacks
 - preventing 537
- DOS prompt 264
- drop box 205
 - defined 582
- DSFFPlugin.plist file 115
- dsimportexport 555
 - exporting users and groups 184
 - export parameters 184

- importing users and groups 181
- import parameters 181
- status information and logs 179
- Dynamic Host Configuration Protocol. *See* DHCP
- dynamic IP address
 - defined 583
- dynamic IP addresses 476

E

- eMac 487
- email client software 406
- email service. *See* mail service
- enabling 346
- error logs 228, 233
- Ethernet networks 488
- Ethernet ports 489, 502
- everyone
 - access privileges 207
 - defined 583
- explicit privileges 206
- export
 - defined 583
- extensions, filename 248

F

- file compression 247–248
- file name extensions 248
- files
 - compressed 247
 - conversion in FTP 247–248
- file services
 - See also* Apple Filing Protocol (AFP),
Windows service, Network File System
(NFS) service, File Transfer Protocol
(FTP)
 - applications for 221
 - more information 265
 - options 48
 - planning 221–223
 - security guidelines 222
 - setup overview 223
 - types of 221
- file sharing
 - about 48

- key features of 44
- organizing 210
- planning 209–211
- security 210
- setup overview 208–209

File Transfer Protocol (FTP) 247–248

- about 50, 244
- anonymous FTP 249
- connections 264
- custom root 248
- defined 583
- guest access 249
- planning 248–249
- security of 244
- setting up sharing 213
- setup overview 249–250
- specifications 248
- user environments 245–247

filters

- defined 583
- editing 532
- examples 529–530
- junk mail 373–375

filters, IP

- adding 531
- described 527–528
- problems locating 543

Finder workgroup 436

firewall

- defined 583
- filtering SMTP connections 401
- sending mail through 390

firewall, NFS 256

Firewall service 525–543

- about 525
- adding filters 531
- Any Port filter 537
- benefits 526
- blocking multicast services 536
- configuring 530, 533–534
- creating filters 532
- default filter 537
- described 525
- editing filters 532
- example filters 529–530

- filtering UDP ports 535–536
 - filters 527–529
 - IP address precedence 529
 - IP filter rules 538–540
 - logs, setting up 534–535
 - managing 531–538
 - more information 543
 - multiple IP addresses 529
 - NetInfo Access, controlling 536
 - port reference 540–542
 - preparing for setup 527–529
 - preventing denial-of-service attacks 537
 - problems with 543
 - setting up 530–531
 - solving problems 543
 - starting 531
 - starting automatically 531
 - stopping 531
 - uses for 526
 - viewing logs 533
 - folder access privileges 444
 - folders
 - Documents folder 341
 - fonts
 - adding to client systems via network 208
 - FTP
 - defined 583
 - FTP passive mode 265
 - FTP root and share points user environment 245
 - FTP servers
 - security of 244, 249
 - FTP service 244–248
 - Access settings 251
 - Advanced settings 252
 - anonymous 253
 - anonymous uploads folder 253
 - authentication method 254
 - custom root 253
 - described 221, 244–248
 - displaying messages 255
 - displaying user messages 255
 - General settings 250
 - Logging settings 251
 - preparing for setup 248
 - README messages 255
 - security limitations 50
 - setup overview 256–257
 - solving problems 264
 - specifications 248
 - starting 252
 - stopping 252
 - user environment 254
 - viewing logs 254
- G**
- Getting Started With Mac OS X Server 41
 - group
 - defined 583
 - group accounts
 - about 127
 - access privileges 125, 127, 206
 - adding users 148, 168
 - administering 165
 - automatic group directory 171
 - changing 167
 - creating in Mac OS X Server directory
 - domain 165
 - creating in read-write LDAPv3 domains 166
 - defined 121
 - deleting 173
 - directories for 128, 170
 - in directory domains 71
 - finding 173
 - group ID 170
 - names for 169
 - planning 136
 - predefined, list of 131
 - read-only 167
 - removing users 149, 168
 - reviewing memberships 149
 - using presets 177
 - where they're stored 165
 - group directories 171
 - group directory
 - defined 583
 - group names 169
 - group preferences
 - managing, Mac OS X 286
 - groups
 - characteristics of 127

- data types 580
- preparing for setup 135
- guest (predefined group account) 131
- guest access
 - allowing 238
 - FTP service 249
 - restricting 210
 - Windows 263
 - Windows services 243
- guest accounts
 - access guidelines 210
 - security guidelines 222
- guest computer
 - defined 583
- guests
 - restricting access 210
- guests users
 - limiting connections 227
- guest user account, Mac OS 9 and 8 429
- guest users
 - about 129
 - accessing Apple file service 234
 - access privileges 129
 - defined 583
 - described 210
 - limiting connections 234
 - maximum connections 227, 234
 - services available to 154

H

- hard disk
 - capacity of 488
- help 41
- hierarchies. *See* directory domain hierarchies
- home directories
 - about 126
 - advanced 163
 - AFP share points 160
 - and disk quotas 164
 - choosing a protocol 160
 - creating folders 161
 - default 165
 - defined 583
 - deleting 165
 - distributing 156

- for local users 162
- for network users 163
- for users in existing directory servers 157
- Macintosh Manager and 422
- moving 165
- NFS share points 160
- Open Directory and 71
- planning 136
- solving problems 204
- storage of 155
- Home Directory and FTP Root user
 - environment 246
- Home Directory Only user environment 247
- HTML
 - defined 583
- HTTP
 - defined 583
- httpd.conf file 358
- httpd_macosxserver.conf file 355, 360
- Hypertext Markup Language (HTML)
 - defined 583
- Hypertext Transfer Protocol (HTTP)
 - defined 583

I

- IANA
 - defined 584
- IANA registration 517
- iBook 487
- ICMP
 - defined 584
- idle user
 - defined 584
- IGMP
 - defined 584
- IGMP packets
 - blocking 536
- iMac 487
- IMAP
 - about 371
 - administrator access 394
 - case-sensitive folders 386
 - connections per user 386
 - ports 387, 394
 - response name 386

- secure authentication 385
 - settings 385–387
 - terminating idle connections 387
 - IMAP (Internet Message Access Protocol)
 - defined 584
 - importing and exporting
 - creating character-delimited files 187
 - creating XML files using AppleShare IP 186
 - creating XML files using Server Admin 186
 - file formats supported 179
 - from Workgroup Manager 181
 - Password Server users 197
 - with Workgroup Manager 179
 - importing and exporting users and groups 178
 - information, finding more 41
 - installer 558
 - Internet and Web services
 - key features of 46
 - Internet Assigned Numbers Authority (IANA)
 - defined 584
 - Internet Control Message Protocol (ICMP)
 - defined 584
 - Internet Gateway Multicast Protocol *See* IGMP
 - Internet Group Management Protocol (IGMP)
 - defined 584
 - Internet Message Access Protocol (IMAP)
 - defined 584
 - Internet Message Access Protocol (IMAP). *See* IMAP
 - Internet Protocol (IP)
 - defined 584
 - Internet servers. *See* Web servers
 - Internet Service Provider (ISP)
 - defined 584
 - IP
 - defined 584
 - IP address, static
 - defined 588
 - IP addresses
 - assigning 477
 - DHCP and 475
 - DHCP lease times, changing 480
 - dynamic 476
 - dynamic allocation 476
 - leasing with DHCP 475
 - multiple 348, 529
 - precedence in filters 529
 - ranges 528
 - reserved 477
 - setting up for ports 348
 - setting up multiple on port 348
 - static 476
 - IP failover 567–571
 - configuring 569
 - defined 46
 - enabling 569
 - requirements 567
 - scripts 570
 - IP Filter module 538–540
 - IP filter rules 538
 - IP filter service 263, 265
 - IP firewall service
 - about 54
 - ipfw command 538–540
 - ISP
 - defined 584
- J**
- Java
 - JavaServer Pages (JSP) with Tomcat 347
 - servlet (with Tomcat) 347
 - Tomcat and 347
 - junk mail 373–375, 398–402
 - approved servers list 374, 398
 - blacklisted servers 375, 401
 - disapproved servers list 375, 399
 - ORBS server 375, 401
 - rejected SMTP servers 375, 399
 - restricted SMTP relay 374, 375, 398, 401
 - reverse DNS lookup 375, 399
 - SMTP authentication 374, 375, 389
- K**
- Kerberos
 - enabling for AFP 200
 - enabling for FTP 200
 - enabling for login window 200
 - enabling for mail 200
 - enabling for Telnet 201

- integrating Mac OS X with Kerberos server 199
- Macintosh Manager 464
- mail service authentication 381
- services supporting 197
- solving problems 204
- understanding 198
- using 197
- Kerberos authentication
 - Apple file service 224
 - FTP service 248, 254
- knem (predefined group account) 131

L

- LDAP
 - defined 584
 - DHCP and 479
- LDAP Bind authentication 201
- LDAP server
 - address via DHCP 479
- LDAPv2
 - access settings 107
 - adding servers 106
 - configuring 106–110
 - data mappings 108
 - enabling and disabling 93
 - search bases 108
 - search policies and 107
 - setting up 106
- LDAPv3
 - adding server configurations 98
 - automatic search policy and 84
 - changing server configurations 99
 - configuring 97–103
 - connection settings 100
 - creating group accounts 166
 - creating user accounts 138
 - deleting server configurations 100
 - duplicating server configurations 99
 - enabling and disabling 94
 - populating with data 103
 - port configuration 101
 - search policies and 99, 100
 - shared domains 83
 - showing and hiding configurations 97

- SSL encryption 101
- lease period
 - defined 584
- Lightweight Directory Access Protocol (LDAP)
 - defined 584
- Lightweight Directory Access Protocol (LDAP).
 - See* LDAPv2, LDAPv3
- Line Printer Remote (LPR)
 - defined 584
- load balancing
 - defined 584
 - NetBoot and 504–505
- load distribution 523
- local directory domain
 - in automatic search policy 83
 - information storage 74
 - listing users and groups 174
 - NetInfo 111
 - search policy 96
- local domain
 - defined 584
- local home directory
 - defined 584
- log files
 - access logs 227
 - error logs 228, 233
- logging in
 - solving problems 203, 204
- logging items
 - DHCP activity 478
 - settings for 546
 - settings for Windows 239
- login settings 146
- log rolling scripts 555
- logs
 - access 352
 - Apple file service 227
 - Apple file service access 233
 - Apple file service error 233
 - DHCP 480, 483
 - DNS service 519
 - dsimportexport 179
 - error 352
 - Firewall 534
 - Firewall service 533

- FTP 254
 - mail service 404
 - print service 325, 332–334
 - reclaiming disk space 555
 - reclaiming space used by 405
 - Server Monitor 63
 - SLP DA 549
 - SSL 357
 - Web service 348
 - Windows services 243
 - LPR
 - defined 584
- M**
- MacBinary (.bin) format 247
 - machine record
 - for NetInfo binding 113
 - Macintosh Manager 411
 - about 411
 - access privileges 442
 - administrator access to user accounts 464
 - administrator login 425
 - All Other Computers account 452
 - allowing media access 442
 - allowing multiple logins 434
 - allowing screen shots 442
 - allowing system access 434
 - approved items 442
 - changing administrator password 433
 - changing language script 418
 - changing menu access 443
 - checking email automatically 451
 - choosing language 417
 - computer access 454
 - computer checkout 423, 461
 - computer lists 451
 - computer Security settings 456
 - copying Mac OS 8 preferences 464
 - creating administrator accounts 432
 - creating email addresses 455
 - creating shortcuts 438
 - customizing reports 463
 - customizing workgroup panels 460
 - desktop environments 436
 - directory services database 420
 - disabling extensions 459
 - disabling login on a computer 453
 - disconnecting computers automatically 454
 - duplicating workgroups 437
 - finding users 429
 - folder access privileges 444
 - force-quitting applications 459
 - Global CD-ROM settings 465
 - Global settings 462
 - group documents 444
 - hand-in folder 445
 - helper applications 457
 - home directories 413, 422
 - importing user accounts 426
 - importing user information from text 428
 - installing administrator software 415
 - Items settings 438
 - Kerberos verification 464
 - listing available discs 465
 - local users and 461
 - login message 451, 460
 - Login settings 460
 - Mac OS X user access 429
 - managing preferences 422
 - media access 457, 465
 - MMLocalPrefs extension 423
 - modifying workgroups 438
 - more information 473
 - mounting volumes automatically 446
 - Multi-User Items folder 419, 420
 - naming hard disks 455
 - Netboot and 423
 - opening items at startup 450
 - Options settings 449
 - preference storage 422, 423
 - preventing user password changes 464
 - printing 420
 - print quotas 448
 - Privileges settings 440
 - protecting folders 440
 - protecting the desktop 440
 - quitting administrator program
 - automatically 463
 - restricting printer access 448
 - security 418, 462, 463

- setting file-level security 441
- setting idle logout 456
- setting media access 441
- setting preferences 426
- setting storage quotas 435
- setting up 424
- setting up administrator accounts 432
- setting up All Other Users 430
- setting up workgroups 436
- shared folders 443
- share point for 419
- solving problems 470–472
- switching servers 459
- synchronizing clocks 455
- synchronizing user database 435
- system access printer 449
- update package 417
- user account template 426
- user information storage 421
- user settings, advanced 434
- user settings, basic 433
- users working offline 458
- using server administrator accounts 432
- viewing reports 463
- wireless service 462
- workgroup printers 447
- Workgroup settings 454
- workgroup template 437
- Macintosh Manager administrator 431, 432
- changing password 433
- Macintosh Manager application
 - opening 62
- Macintosh Manager User predefined
 - account 130
- Macintosh-specific Web modules 365
- Mac OS systems
 - cross-platform guidelines 236
- Mac OS X
 - data requirements 573
- Mac OS X Server
 - applications summary 56
 - individual services of 46
 - key features of 43
 - more information 64
 - ports used by 540–542
 - resources 64
 - setting up 41
 - shared directory domains 75–78
- Mac OS X systems 540–542
- mail
 - disabling for user 150
 - enabling user options 150
 - forwarding for user 151
 - redirecting 517
- mail (predefined group account) 131
- MailAttribute data type, format of 577–579
- mail database
 - about 373
 - administrator access 394
 - backing up 408
 - cleaning up 395, 408
 - converting 393
 - location of 394
- mail exchange (MX) records. *See* MX records
- Mail Exchange. *See* MX
- mail exchange record (MX)
 - defined 585
- mail exchangers 516
- mail host 372
 - defined 585
- mail servers 517
- mail service
 - administrator access 394
 - alternate transfer agent 391
 - APOP authentication 384
 - approved servers list 374, 398
 - authentication 381, 384, 385, 389
 - backing up 408
 - blacklisted servers 375, 401
 - blind carbon copies (BCC) 382
 - case-sensitive IMAP folders 386
 - client settings for 406
 - configuration storage 376
 - connected users 404
 - database 373, 393–396
 - database cleanup 408
 - deleted users, removing mail of 395
 - deleting mail automatically 383, 394
 - disapproved servers list 375, 399
 - DNS cache 397

- DNS lookup for 396
- domain name list 381
- features not supported 376
- features of 369
- filtering SMTP connections 401
- forwarding undeliverable mail 402
- general settings 380–382
- HELO command 400
- idle IMAP connections, terminating 387
- IMAP (Internet Message Access Protocol) 371, 385–387, 394
- IMAP authentication 385
- IMAP connections per user 386
- IMAP port 387
- IMAP response name 386
- incoming mail 378, 382–387
- junk mail prevention 373–375, 398–402
- Kerberos authentication 381
- key features of 51
- limiting delivery attempts 402
- limiting incoming message size 383
- logs 404, 405
- maintenance 379
- message storage 373, 393–396
- monitoring 404
- more information 408
- MX records 372, 377, 381, 396
- network settings 396–397
- new mail notification 383
- NotifyMail protocol 383
- ORBS server 375, 401
- outgoing mail 378, 387–393, 402–403
- performance tuning 407
- planning 379
- POP (Post Office Protocol) 370, 384–385
- POP port number 385
- POP response name 384
- postmaster account 379, 402, 403
- protocols 370, 382
- rejected SMTP servers 375, 399
- relay via another server 389
- reporting undeliverable mail 402, 403
- resources 408–409
- restricted SMTP relay 398
- reverse DNS lookup 375, 399
- sending nonlocal mail 388
- sending only local mail 388
- Sendmail 371, 373, 392
- setup overview 377–379
- SMTP (Simple Mail Transfer Protocol) 371, 389–393, 401
- SMTP alternate 391
- SMTP authentication 389
- SMTP ports 391
- SMTP relay for backup server 401
- SMTP response name 390
- SSL (Secure Sockets Layer) 372
- starting and stopping 378, 380
- status 403–405
- suspending outgoing mail 388
- timeouts 397
- tools overview 376
- undeliverable mail 402–403
- user accounts 404, 407
- user account settings for 373, 379, 405
- using DNS service with 516
- virtual host list 381
- mail settings
 - creating for users 127
- mail transfer agent (MTA) 371, 391
- mail transfer agent (MTSA)
 - defined 585
- managed client
 - defined 585
- managed preferences
 - defined 585
- managed preferences. *See* preference management
- Managed Preferences folder 466
 - Forced Preferences folder 467
 - Initial Preferences folder 466
 - Initial Preferences folder, exceptions 467
 - Preserved Preferences folder 468
- managed users
 - about 128
- management information bases (MIBS)
 - defined 585
- mapping
 - group records 580
 - Mac OS X data types 573

- user records 574–577
- mappings
 - BSD configuration files 116
 - LDAPv2 108
 - LDAPv3 101
- MBONE
 - defined 585
- messages, mail. *See* mail service
- MIBS
 - defined 585
- MIME
 - defined 585
 - mappings 343
 - server response, setting 356
 - suffixes 340
 - type mapping 340
 - types 343
 - Types pane 343
 - understanding 340
 - Web server responses 340
- MIME (Multipurpose Internet Mail Extension) 340–341
- MMLocalPrefs extension 423
- mod_auth_apple module 365
- mod_hfs_apple module 366
- mod_machbinary_apple module 365
- mod_perl module 366
- mod_redirectcgi_apple module 366
- mod_sherlock_apple module 365
- MTA
 - defined 585
- MTA (mail transfer agent) 371
- multicast backbone (MBONE)
 - defined 585
- multicast DNS 72
- multicast services
 - blocking 536
- multihoming
 - changing priority of network connections in Mac OS X 260
 - defined 585
- Multipurpose Internet Mail Extension (MIME)
 - defined 585
- Multipurpose Internet Mail Extension. *See* MIME
- MX (Mail Exchange) Records
 - defined 585
- MX (Mail Exchange) records 517, 518
- MX hosts 516
- MX records 372, 377, 381, 396
- mysql (predefined group account) 131
- MySQL Manager 367, 565
- MySQL module 367
- My SQL Server predefined account 130

N

- named.conf file 520
- name servers 516
- NAT (Network Address Translation) 390
- Neighborhood settings 239
- NetBIOS
 - defined 585
- NetBoot 491
 - “system-less” clients 506
 - about 52
 - administration tools for 62
 - administrator requirements 486
 - AirPort 493
 - applications and files for 485
 - Boot Server Discovery Protocol (BSDP) 491
 - capacity planning 488
 - client computer requirements 487
 - client computers 505, 506
 - configuring 501
 - creating Mac OS X disk image 496
 - default disk image 500
 - disabling disk images 502
 - disabling on Ethernet ports 502
 - disk images 492
 - enabling 501, 502
 - filtering clients 503
 - hard disk name in 455
 - image folders
 - image folders, NetBoot 489–490
 - installing Classic 497
 - key features of 485
 - load balancing 504–505
 - monitoring Mac OS 9 clients 503
 - monitoring Mac OS X clients 503
 - network requirements 488
 - property lists 490

- security 493
- server requirements 486
- setting up Mac OS 9 disk image 497, 498
- setting up on Mac OS X Server 496
- setup overview 493–496
- shadow images 492
- solving problems 507–508
- starting up on client computers 495
- Trivial File Transfer Protocol (TFTP) 492
- updating Mac OS X disk images 503
- updating Startup Disk control panel 505
- viewing client lists 483
- NetBoot client computers 506
- NetBoot Desktop Admin 490
- NetBoot server
 - defined 585
- NetInfo 264
 - See also* directory domains
 - access through firewall 536
 - automatic search policy and 84
 - binding 111, 482
 - child 110
 - client access 482
 - configuring 110–114
 - data, changing 114
 - data, viewing 114
 - defined 585
 - directory service protocol 74
 - enabling and disabling 94
 - information storage 114
 - machine record 113
 - parent 110
 - port configuration 113
 - shared domains 83, 110
 - UNIX tools for 114
- NetInfo Manager application
 - data, viewing 114
 - machine records, adding 113
 - ports, configuring 113
- network
 - adding fonts to client systems 208
- network (predefined group account) 131
- network authentication protocols 88
- Network Basic Input/Output System (NetBIOS)
 - defined 585
- Network File Service (NFS)
 - security limitations 222
- Network File System (NFS)
 - defined 586
 - exporting share points 215
 - home directories in 160
 - resharing in AFP 215
 - setting up share points 213
- Network File System (NFS) service
 - about 49
 - security limitations 49
- Network Globe
 - contents 207–208
 - folders in 208
 - share points 208
- Network Image Utility 489
 - creating disk image 511
 - creating Mac OS X disk image 496
- Network Install
 - about 53
 - about packages 509
 - applications and files for 509
 - creating custom packages 512
 - creating disk image 511
 - enabling disk images 513
 - key features of 509
- Network Install application 62
- network installation
 - defined 586
- network library folder
 - system resources 208
- Network Neighborhood 263
 - connecting to server without 262
 - connecting to service with 262
- networks
 - management resources 64
 - private 523–524
 - scopes 546, 546–547
 - sharing printer queues over 317
 - TCP/IP networks 523–524
- Network Service Locator (NSL)
 - defined 586
 - registering Apple file servers 231
- network services
 - assigning to scopes 547

- discovery protocols 72
- networksetup 562
- NFS
 - defined 586
- nfsd daemons 257
 - defined 586
- NFS service
 - about 256
 - configuring settings 257
 - described 221
 - monitoring 258
 - planning 256
 - stopping 258
 - uses for 256
- nobody (predefined group account) 131
- nogroup (predefined group account) 131
- None privilege 205
- NotifyMail protocol 383
- NSL
 - defined 586

O

- online help 41
- Open Directory
 - See also* directory services
 - access privileges and 71
 - authentication 67, 70
 - automount share points and 71
 - backing up 119
 - BSD configuration files and 115
 - compared to UNIX systems 69
 - configuring protocols 93
 - data requirements 573
 - defined 586
 - group accounts and 71
 - home directories and 71
 - information management 70, 73
 - information storage in 65, 72
 - key features of 47
 - mail settings and 71
 - overview 45
 - protocols supported 74
 - quotas and 71
 - searching non-Apple domains 78
 - search policies 82–84

- service discovery and 72
- UNIX heritage 67
- uses of 70–71
- Open Directory Assistant
 - about 92
 - configuring directory domain 92
 - connecting to server 92
 - creating shared NetInfo domain 111
 - deleting shared directory domain 93
- Open Directory Assistant application 58
- Open Directory domains
 - See also* directory domains, LDAPv3, NetInfo
 - deleting 93
 - setting up 92
- Open Directory Password Server. *See* Password Server
- OpenLDAP
 - directory service protocol 74
- open relay
 - defined 586
- Open Relay Behavior-modification System (ORBS)
 - defined 586
- open source modules 366–367
- operator (predefined group account) 131
- ORBS
 - defined 586
- ORBS servers 375, 401
- owner
 - defined 586
- owner privileges 206

P

- Package Maker application 62
- packages 509
- Panels workgroup 436
- parent computer
 - defined 586
- parent NetInfo domain 110
- passwords
 - administrator 137
 - file servers 263
 - migrating 193
 - problems with readable 194
 - root 137

- root user 137
 - validating 189
 - validation strategies 189
- Password Server 264
 - administration 196
 - authentication protocols 195
 - authentication with 87
 - backing up 201
 - database contents 88
 - enabling for a user 196
 - monitoring 197
 - protocols supported 88
 - recommended for Windows 236
 - securing 197
 - security benefits 66
 - security features 195
 - security guidelines 89
 - setting up 92
 - setup 196
 - solving problems 203
 - tools for managing 89
 - Windows validation 202
- password validation
 - authentication authority attribute 192
 - basic strategy 193
 - choosing a password 192
 - for Windows 236
 - Kerberos 197
 - options 47, 189
 - Password Server strategy 195
 - pros and cons 191
 - strategies 123
 - Windows 202
- percent symbol
 - defined 586
- performance
 - mail service 407
- Perl
 - mod_perl 366
- PHP 366
 - defined 586
 - enabling 357
 - Hypertext Preprocessor *See* PHP
- PHP Hypertext Preprocessor (PHP)
 - defined 586
- PHP module 366
- POP
 - about 370
 - authentication 384
 - port number 385
 - response name 384
 - settings 384–385
- POP (Post Office Protocol)
 - defined 586
- port 548 263
- portable computers, Mac OS 9 and 8 461
 - wireless service 462
- portable computers, Mac OS X
 - as guest computers 280
 - individual 280
 - managing preferences 279
 - shared 280
- ports
 - Ethernet ports 489
 - IMAP mail administrator 394
 - IMAP mail service 387
 - IP addresses 348
 - Mac OS X computers 540–542
 - POP mail service 385
 - SMTP 391
 - SMTP mail service 391
 - TCP ports 540–541
 - UDP ports 542
- Postfix program, configuring 371
- postmaster mail account 379, 402
- Post Office Protocol (POP)
 - defined 586
- Post Office Protocol (POP). *See* POP
- PowerBook (FireWire) 487
- PowerBook G4 487
- Power Mac G4 487
- Power Mac G4 Cube 487
- Power Macintosh G3 (blue and white) 487
- predefined accounts
 - defined 586
- preference cache
 - about 283
 - how to empty 283
 - updating 283
- preference management, Mac OS 9 and 8 466

- preference management, Mac OS X
 - about 284
 - Applications Items settings 288
 - Applications preference 288
 - Applications System Preferences settings 290
 - Classic Advanced preferences 292
 - Classic preferences 291
 - Classic settings 291
 - computer preferences 286
 - disabling 287
 - Dock Display settings 294
 - Dock Items settings 295
 - Dock preference 294
 - editing multiple records 287
 - Finder Commands settings 299
 - Finder preference 296
 - Finder Views settings 302
 - group preferences 286
 - Internet Email settings 304
 - Internet preference 304
 - Internet Web settings 304
 - local user accounts 279
 - Login Items settings 307
 - Login preference 305
 - Login Window settings 305
 - Media Access Disk Media settings 308
 - Media Access Other Media settings 309
 - Media Access preferences 308
 - options 284
 - preference cache 283
 - Printing preferences 311
 - Printing Printer List settings 311
 - Startup settings 291
 - user preferences 285
- preferences, Mac OS 8 464
- preferences cache, defined 587
- presets
 - changing 178
 - creating for groups 177
 - creating for users 176
 - defined 176, 587
 - deleting 178
 - renaming 178
 - using to create new accounts 177
- primary group 129
 - defined 148, 587
 - group ID of 148
- primary group ID
 - defined 587
- Print Center
 - adding print queue from Open Directory domain 323
 - adding print queue using AppleTalk 323
 - adding print queue using LPR 323
- printer sharing
 - key features of 44
- print jobs
 - deleting 332
 - holding 330
 - holding new 331
 - monitoring 329
 - prioritizing 331–332
 - restarting 330
 - stopping 330
- print logs
 - deleting 334
 - managing 332–334
- print queues
 - about 315
 - adding from Open Directory domain 323
 - adding in Mac OS X using AppleTalk 323
 - adding in Mac OS X using LPR 323
 - adding to Open Directory domains 321
 - configuring 320
 - default 329
 - deleting 329
 - holding 327
 - monitoring 326
 - reconfiguring 327
 - renaming 328
 - restarting 327
- print quotas
 - enforcing 322
 - managing 332
 - setting for Mac OS 9 and 8 clients 448
 - setting up 322
- print service
 - about 315
 - adding printers 320
 - applications for 315

- key features of 50
- monitoring 325
- printers supported 316
- protocols supported 317
- setting up 319
- setting up Mac OS 8 and 9 clients 324
- setting up Mac OS X clients 323
- setting up on clients 323
- setup overview 317–318
- solving problems 334–335
- starting automatically 326
- stopping 326
- UNIX clients 325
- Windows clients 325
- print settings
 - for users 151
- privileges. *See* access privileges
- problems. *See* troubleshooting
- Property List Editor
 - editing BSD configuration files with 116
 - editing DSFFPlugin.plist 116
 - installing 116
- protocols
 - See also* specific protocols
 - directory services 93
 - mail service 370–371
 - Open Directory 93
 - service discovery 72
 - SSL and mail service 372
- proxy 345
 - blocking Web sites with 345
- proxy cache
 - enabling 345
- proxy server 345
 - defined 587

Q

- QTSS (QuickTime Streaming Server)
 - defined 587
- QuickTime Broadcaster
 - about 55
- QuickTime Streaming Server
 - privileges 206
- QuickTime Streaming Server (QTSS)
 - about 55

- defined 587
- quotas
 - about 127
 - disk 164
 - mail 151
 - print 152
 - user settings 71

R

- Read & Write privileges 205
- README messages, for FTP 255
- Read Only privileges 205
- realm, WebDAV
 - defined 590
- realms, WebDAV 339
- Real-Time Streaming Protocol (RTSP)
 - defined 587
- Real-Time Transport Protocol (RTTP)
 - defined 587
- record types
 - about 71
 - adding 102
 - group 580
 - LDAPv2 108
 - LDAPv3 101
 - user 574–577
- remote administration 58
 - Directory Access application 118
- Rendezvous 72
 - defined 587
 - enabling and disabling for Open Directory 94
- reports
 - Macintosh Manager 463
- Request for Comments (RFC) documents 409
- resources
 - Apache Web server 64
 - file services 265
 - Mac OS X Server 64
 - mail service 408–409
 - network management 64
 - Web service 367
- Restricted Finder workgroup 436
- RFC (Request for Comments) documents 409
- root
 - password 137

- root domain 77, 111
 - See also* shared directory domains
 - root password 137
 - root user account
 - backing up 202
 - round robin 523
 - routers 546
 - RTSP
 - defined 587
 - RTTP
 - defined 587
 - rules, IP filter 538–540
- S**
- Samba 235
 - SASL (Simple Authentication and Security Layer) 88
 - schema, directory domain. *See* mappings
 - scopes, network 546, 546–547
 - screen shots 442
 - scripts *See* CGI scripts
 - search bases
 - BSD configuration files 116
 - LDAPv2 108
 - LDAPv3 101
 - search path directory domains
 - listing accounts in 174
 - search policies 202
 - about 48, 82–83
 - adding Active Directory server to 105
 - adding LDAPv2 server to 107
 - adding LDAPv3 server to 99, 100
 - authentication 94
 - automatic 83, 95
 - custom 84, 95
 - local domain only 96
 - setting up 94–95
 - user accounts in 122
 - secure shell (SSH) command 553
 - Secure Sockets Layer (SSL)
 - defined 588
 - Secure Sockets Layer. *See* SSL
 - Secure Sockets Layer. *See* SSL
 - security
 - access privilege guidelines 210
 - file service guidelines 222
 - FTP servers 244, 249
 - key features of 44
 - limitations of NFS 222
 - Macintosh Manager 418
 - NetBoot 493
 - NFS 256
 - NFS exports and 256
 - NFS limitations 210
 - passwords 194
 - Password Server 89
 - root password 137
 - of server hardware 87, 89
 - WebDAV 339
 - Web sites 340
 - Sendmail program 371, 391, 392
 - mail folder 373
 - Sendmail User predefined account 130
 - server administrators
 - using Macintosh Manager accounts 432
 - Server Assistant application 58
 - server management
 - more information 64
 - Server Message Block (SMB)
 - defined 588
 - setting up sharing 212
 - Server Message Block (SMB). *See* SMB
 - Server Monitor application
 - connecting to server 62
 - task summary 62
 - servers
 - Apache Web server 64, 338
 - enabling SSL on 363
 - equipment for 92
 - file servers 263
 - location for 92
 - name servers 516
 - ORBS servers 375
 - proxy servers 345–346
 - security of 87, 89
 - Windows file servers 237
 - WINS servers 240
 - Server Settings
 - adding printers to queue 320

- adding print queues to Open Directory domains 321
- administrator access to mail database 395
- allowing guest access to Apple file service 234
- allowing guest access to Windows services 243
- alternate mail transfer agent 391
- APOP authentication 384
- Apple file service Access settings 226
- Apple file service automatic startup 231
- Apple file service General settings 225
- Apple file service Idle Users settings 228
- Apple file service Logging settings 227
- approved mail servers list 398
- archiving Apple file service logs 233
- archiving print logs 333
- assigning Windows server to workgroup 244
- automatically disconnecting users from Apple file service 234
- blacklisted mail servers 401
- blind carbon copies (BCC), configuring 382
- blocking Web sites with proxy server 345
- CGI script, enabling 355
- changing Apple file server name 231
- changing print job priority 331
- changing print queue quotas 332
- changing Windows server name 241
- configuring NetBoot 501
- configuring print queues 320
- creating Apple file service login greeting 234
- creating SLP DA scopes 546
- custom FTP root 253
- default NetBoot disk image 500
- deleting DHCP subnets 480
- deleting mail automatically 383, 394
- deleting print jobs 332
- deleting print queues 329
- denial-of-service attacks, preventing 537
- deregistering a service with SLP DA 549
- DHCP client list 481
- DHCP logs 480, 484
- DHCP subnet IP address lease times, changing 480
- DHCP subnets, creating 481
- DHCP subnets, settings 482
- disabling DHCP subnets 483
- disabling NetBoot disk images 502
- disapproved servers list 399
- disconnecting users from Apple file service 233
- DNS lookup for mail service 396
- DNS options for DHCP subnets 482
- DNS server for DHCP clients 479
- DNS Service, starting and stopping 519
- enabling AppleTalk browsing on Apple file service 232
- enabling disk images 514
- enabling NetBoot 502
- enabling NetBoot disk images 502
- enabling SSL for Web service 346
- enabling WebDAV 346
- enabling Web site 350
- enabling web site logs 352
- enabling Windows service domain browsing 242
- enforcing quotas for print queues 322
- filtering NetBoot clients 504
- filtering SMTP connections 401
- filtering UDP ports 536
- finding Windows server workgroup name 241
- Firewall, configuring 534
- Firewall, starting and stopping 531
- Firewall default filter 537
- Firewall filters, creating 532
- Firewall filters, editing 532
- Firewall filters, finding 533
- Firewall logs 534
- Firewall service, configuring 530
- FTP Access settings 251
- FTP Advanced settings 252
- FTP authentication 254
- FTP General settings 250
- FTP Logging settings 251
- FTP logs 254
- FTP user environment 254
- FTP user messages 255
- holding new print jobs 331
- holding print jobs 330

- holding print queues 327
- IMAP authentication 385
- IMAP case-sensitive folders 386
- IMAP connections per user 386
- IMAP ports 387
- IMAP response name 386
- Kerberos for mail service 381
- LDAP server address via DHCP 479
- limiting Apple file service connections 232
- limiting connections to Windows services 242
- limiting incoming message size 383
- limiting mail delivery attempts 402
- logging SLP DA debugging messages 549
- mail database location 394
- mail service, starting and stopping 380
- mail service DNS cache 397
- mail service timeouts 397
- mail service virtual host names 381
- modifying MIME type mappings 343
- monitoring print jobs 329
- NetInfo access through Firewall 536
- NetInfo options for DHCP subnets 482
- new mail notification 383
- NFS settings 257
- performance cache for Web site 352
- POP port number 385
- POP response name 384
- reconfiguring print queues 327
- registering Apple file server with NSL 231
- registering a service with SLP DA 548
- registering with WINS server 242
- renaming print queues 328
- reporting undeliverable mail 402
- restarting print jobs 330
- restarting print queues 327
- sending nonlocal mail 388
- sending only local mail 388
- server response for MIME types 356
- setting access port for Web site 351
- setting default print job priority 331
- setting default Web page 351
- setting up anonymous FTP 253
- setting up persistent connections 344
- SLP DA log options 549
- SLP DA scopes, creating 548
- SLP DA scopes, viewing 547
- SLP DA service, starting and stopping 547
- SMTP authentication 389
- SMTP name matches IP address 400
- SMTP ports 391
- SMTP relay, restricting 398
- SMTP relay for backup server 401
- SMTP relay via another server 390
- SMTP response name 390
- SMTP servers, rejecting 399
- specifying default print queue 329
- SSL, enabling 363
- SSL, setting up 357
- starting Apple file service 229
- starting DHCP 478
- starting FTP service 252
- starting or stopping Web service 343
- starting print service automatically 326
- starting Tomcat 347
- starting Web service automatically 343
- starting Windows services 240
- stopping Apple file service 230
- stopping DHCP 478
- stopping FTP service 253
- stopping print service 326
- suspending outgoing mail 388
- terminating idle IMAP connections 387
- turning on Apple file service access logs 232
- undeliverable mail, forwarding 402
- undeliverable mail, reporting 403
- viewing client lists 483
- viewing Web service status 348
- WebDAV, enabling 353
- WebDAV realms, setting up 353
- Web site indexing, enabling 353
- Web sites, monitoring 356
- Windows services automatic startup 241
- Windows services General settings 237
- Windows services Logging settings 239
- Windows services logs 243
- Windows services Network Neighborhood settings 239
- Server Settings application
 - connecting to server 60

- opening within Workgroup Manager 60
- populating Active Directory domains
 - with 105
 - populating LDAPv3 domains with 103
- Server Side Includes *See* SSI
- Server Status
 - Apple file service logs 230
 - Apple file service status 230
 - disconnecting users from Windows services 243
 - DNS log, viewing 519
 - DNS service status 519
 - DNS usage statistics 520
 - mail service 404, 405
 - monitoring Mac OS 9 NetBoot clients 503
 - monitoring Mac OS X NetBoot clients 503
 - monitoring NFS 258
 - monitoring print queues 326
 - monitoring print service 325
 - monitoring Windows services 241
 - sending messages to Apple file service users 235
 - SLP DA logs, viewing 549
 - viewing print logs 333
 - viewing Web service logs 348
- Server Status application
 - directory services information 119
 - task summary 61
- service discovery 72
- Service Location Protocol (SLP)
 - about 54
- Service Location Protocol (SLP). *See* SLP
- Service Location Protocol (SLP) Directory Agent (DA)
 - defined 588
- Service Location Protocol Directory Agent *See* SLP DA
- services
 - data items used by 573–574
- settings
 - logging 546
 - logging for Windows services 239
 - MIME types 343
 - Web service 342–349
 - Web sites 349–358
- Shadow Images 492
- shared directory domains
 - deleting 93
 - information storage 75
 - NetInfo 110, 111
 - network printing and 76
 - resources in 77
- share point
 - defined 48
- share points
 - automounting 207, 214
 - changing owner and privileges 217
 - changing protocols 218
 - creating 211
 - defined 205
 - deleting NFS client 218
 - drop box 218
 - for Windows users 236
 - making unavailable 215
 - removing 216
 - resharing NFS mounts 215
 - solving problems 219
 - viewing 216
- sharing
 - stopping 216
- Sherlock
 - AFP and 224
- showmount command 259
- Simple Mail Transfer Protocol (SMTP)
 - defined 588
- Simple Mail Transfer Protocol. *See* SMTP
- Simple Network Management Protocol (SNMP) 566
- SLP
 - discovery protocol 72
 - enabling and disabling for Open Directory 94
- SLP (Service Location Protocol) 226, 231
- SLP DA
 - attributes list 550
 - defined 588
 - more information 550
- SLP DA service 545–550
 - creating scopes 548
 - debugging messages, logging 549
 - deregistering a service 549

- described 545
- managing 547–550
- monitoring 549
- planning 545
- preparing for setup 545
- registering a service 548
- setting up 545–547
- starting 547
- stopping 547
- uses for 545
- viewing scopes 547
- SLP Service
 - managing 547–550
 - starting 547
 - stopping 547
- SMB
 - defined 588
 - enabling and disabling for Open Directory 94
 - Windows protocol 72
- SMB protocol 235
- smmsp (predefined group account) 131
- SMTP
 - about 371
 - alternatives to 371
 - authentication 374, 375, 389
 - filtering connections 401
 - ports 391
 - rejected servers 375, 399
 - relay, restricted 374, 375, 398
 - relay for backup server 401
 - relay via another server 389
 - response name 390
 - settings 389–393
- SMTP (Simple Mail Transfer Protocol)
 - defined 588
- SNMP (Simple Network Management Protocol)
 - defined 588
- softwareupdate 561
- spam
 - defined 588
- spam. *See* junk mail
- specifications
 - Apple file service 224
 - FTP service 248
 - Windows services 236
- spoof 256
- SQL 367
- SquirrelMail *See* WebMail
- SSH
 - key fingerprints 554
- SSH access
 - enabling and disabling 553
- SSH session
 - closing 554
 - executing commands 554
 - opening 553
- SSI
 - enabling 355
- SSL
 - certificate signing request (CSR) 361
 - enabling 363
 - mail service and 372
 - setting up 357, 361
 - Web site certificate 362
- SSL (Secure Sockets Layer)
 - defined 588
 - described 338
 - enabling 363
- SSL (Secure Sockets Layer) service 361–363
- staff (predefined group account) 131
- starting up using N key 507
- Startup Disk control panel, updating 505
- static addressing 487
- static binding, NetInfo 112
- static IP addresses 476
 - defined 588
- Streaming Server Admin application
 - starting 63
 - task summary 63
- subnet 264
- subnet masks 527
- subnets 239, 476
 - creating 476, 477–478, 481
 - defined 588
- sys (predefined group account) 131
- system access printer 449
- System Administrator predefined account 130
- system identifier lights
 - and Server Monitor 63
- System-less clients

- defined 588
- System Preferences
 - setting up multiple IP addresses for a port 348
- System Services predefined account 130
- systemsetup 561

T

- TCP
 - defined 589
- TCP/IP 264
 - private networks 523–524
 - unable to access server over 543
- TCP/IP, for Windows services 262
- TCP ports 540–541
- templates, directory domain. *See* mappings
- Terminal application 258, 539, 552
 - mail database cleanup 395
 - NetInfo command-line tools in 114
 - Sendmail, starting 392
 - SSH command 553
- time-to-live (TTL)
 - defined 589
- Tomcat 366
 - defined 589
 - Java and 347
 - Java servlet 347
 - JSP (JavaServer Pages) 347
 - starting 347
- Tomcat module 366
- TP service
 - anonymous 249
- Transmission Control Protocol (TCP)
 - defined 589
- Trivial File Transfer Protocol (TFTP) 492
- troubleshooting
 - Apple file servers 263
 - Apple file service 263
 - Firewall service 543
 - FTP 264
 - IP filters 543
 - NetBoot 507–508
 - print service 334–335
 - share points 219
 - users and groups 202

- Web service 364
- Windows services 263

- TTL
 - defined 589
- tty (predefined group account) 131
- tunneling 546

U

- UDP
 - defined 589
- UDP (User Datagram Protocol) 258
- UDP Ports
 - filtering 535
- UDP ports 542
- undeliverable mail
 - forwarding 402
 - limiting delivery attempts 402
 - reporting to postmaster 402, 403
- Unicode
 - defined 589
- Uniform Resource Locator (URL)
 - defined 589
- Universal Serial Bus (USB) 316
 - defined 589
- UNIX
 - commands, understanding 553
 - finding help 553
- UNIX systems
 - BSD configuration files 74
 - compared to Open Directory 67, 68, 69
 - information storage 68, 69
 - tools for NetInfo 114
- unknown (predefined group account) 131
- Unknown User predefined account 130
- Unprivileged User predefined account 130
- unsolicited mail. *See* junk mail
- uploads folder in FTP 253
- URL
 - defined 589
- USB
 - defined 589
- USB (Universal Serial Bus) 316
- user, virtual
 - defined 589
- user accounts

- access privileges 125
- authenticating 123
- authentication 122
- changing 138
- comments 147
- connecting without logging in 123
- creating in Mac OS X Server directory domains 137
- creating read-write LDAPv3 user accounts 138
- defined 121
- defining a user's home directory 161
- deleted, removing mail of 395
- deleting 154
- in directory domains 66–67, 91
- disabling 155
- disabling mail 150
- disk quotas 164
- enabling mail options 150
- finding 173
- forwarding mail 151
- group settings 147
- home directories 126
- how they're used 122
- importing into Macintosh Manager 426
- kinds of 128
- locations of 137
- login settings 146
- Mac OS 9 and 8 420
- mail addresses 407
- mail quotas 127
- mail settings 127, 150, 373, 379, 405
- managed users 128
- managing preferences 270
- naming guidelines 141
- not using a home directory 162
- password validation 189
- postmaster 379
- predefined, list of 130
- presets 176
- print settings 151
- read-only 139
- storing preferences 127
- user and group accounts
 - planning 135
 - role in network 121
 - setup overview 132
- user data
 - how used by server 573
- User Datagram Protocol (UDP)
 - defined 589
- User Datagram Protocol *See* UDP
- user environment in FTP 254
- user environments in FTP 245–247
- user experience
 - Mac OS 9 and 8 desktop 436
- user ID (UID)
 - defined 589
 - guidelines 144
 - network role of 124
 - role in access privileges 125
- user messages
 - FTP 255
- user messages, for FTP 255
- user names
 - defined 589
 - long names 139
 - as mail addresses 407
 - short names 140
- user preferences
 - managing, Mac OS X 285
- Users 364
- users
 - anonymous FTP users 265
 - categories 206
 - characteristics of 122
 - data types 574–577
 - limiting connections 227, 234
 - MailAttribute data type 577–579
 - mail client configuration 406
 - mapping data 573–579
 - preparing for setup 135
 - registered 222
 - unregistered 210
- users and groups
 - importing and exporting 178
 - solving problems 202
- utilities
 - advanced, list of 551
- utmp (predefined group account) 131

uucp (predefined group account) 131

V

virtual hosts
 mail service 381
Virtual Private Network (VPN)
 defined 589
virtual user
 defined 589
VPN
 defined 589

W

Web 365
Web-based Distributed Authoring and Versioning
 See (WebDAV)
Web browsers 339
WebDAV
 defined 590
 privileges 206
WebDAV (Web-based Distributed Authoring and
 Versioning) 346
 defining realms 339
 described 337
 enabling 353
 security 339
 setting access 354
 setting access privileges 339
 setting up 346
 understanding 339
WebDAV realm
 defined 590
WebMail
 about 358–361
 configuring 360–361
 enabling 359
 logging in 359
 mail server and 359
 protocols 359
 security limitations 359
 SquirrelMail 358
Web modules 365–367
 Mac-specific 365
 open-source 366

Web pages
 default 341
Web servers
 Apache Web server 64, 338
 certificate for 362–363
Web Service
 monitoring 348
Web service 337–367
 about 337–367
 configuring 338, 342
 default page 341
 described 337
 Documents folder 341
 key features of 51
 limiting simultaneous 344
 monitoring 348
 more information 367
 MySQL 367
 persistent connections 344
 preparing for setup 338–340
 problems with 364
 resources 367
 secure transactions 338, 361–363
 settings for 342–349
 setting up 341–342
 setting up Web sites 338
 setup overview 341–342
 solving problems 364
 SSL, enabling 346
 starting 343
 stopping 343
 strategies for 338–341
 Tomcat 347
 WebDAV 346
 WebMail, managing 359–361
 Web site privileges 342
Web services
 logs, viewing 348
Web site
 setting up SSL 357
Web Sites 349–358
 monitoring 356
Web sites
 access privileges 340
 Apache Web server 64

- assigning privileges 342
 - connecting to 342
 - connection problems 364
 - default Page 351
 - default page 341
 - default Web Folder 349
 - directory listing 352
 - documents Folder 349
 - enabling 350
 - hosting 339, 342
 - improving performance 351
 - information about 349
 - logs 352
 - MIME, configuring 356
 - security of 340
 - setting access port 351
 - settings for 349–358
 - setting up 338
 - solving problems 364
- wheel (predefined group account) 132
- wildcard
 - defined 590
- Windows clients
 - share points for 210
- Windows file servers 237
- Windows Internet Naming Service (WINS) 235
 - defined 590
 - registering with 242
 - servers 240, 264
- Windows services 235–236
 - Access settings 238
 - assigning server to workgroup 244
 - authentication 236
 - automatic startup 240
 - changing server name 241
 - connecting to server with Network Neighborhood 262
 - connecting to server without Network Neighborhood 262
 - cross-platform guidelines 236
 - described 221
 - disconnecting users 243
 - enabling domain browsing 242
 - finding server workgroup name 241
 - General settings 237
 - guest access 243
 - key features of 49
 - limiting connections 242
 - logging settings 239
 - monitoring 241
 - Network Neighborhood settings 239
 - password validation 236
 - planning 236–237
 - problems with 263
 - registering with WINS server 242
 - Samba 235
 - services supported 235
 - setting up logs 243
 - solving problems 263
 - specifications 236
 - starting 240
 - stopping 240
 - supported in Mac OS X Server 261
 - using TCP/IP 262
- Windows systems
 - cross-platform guidelines 236
- WINS
 - defined 590
- wireless service 281
- workgroup administrator 432
- workgroup management, Macintosh
 - key features of 45, 52
- Workgroup Manager
 - about 267
 - access for users with local accounts 279
 - adding Dock items 295
 - adding to computer accounts 274
 - adding users to groups 168
 - allowing access to local applications 289
 - allowing access to System Preferences 290
 - allowing burning CDs and DVDs 309
 - allowing CD and DVD access 308
 - allowing helper applications 289
 - allowing special actions during restart 292
 - allowing users to control Dock 296
 - approving applications 288
 - authenticating in 59
 - automounting share points 214
 - browsing share point folders 216
 - changing computer accounts 274

- changing group accounts 167
- changing owner and access privileges for share point 217
- changing share points' protocols 218
- changing user accounts 138
- computer access settings 278
- computer account presets 273
- computer accounts, creating 272
- configuring an AFP share point 212
- configuring an FTP share point 213
- configuring an SMB share point 212
- controlling computer access 278
- copying access privileges 217
- creating drop box 218
- creating group accounts 166
- creating LDAPv3 group accounts 166
- creating LDAPv3 user accounts 138
- creating printer list 311
- creating user accounts 137
- deleting computer accounts 276
- deleting computers from accounts 275
- deleting NFS client from share point 218
- disabling preference management 287
- editing multiple users 176
- ejecting media on logout 310
- exporting users and groups in 181
- filtering account lists 175
- hiding "Connect to Server" command 299
- hiding "Go to Folder" command 300
- hiding "Go to iDisk" command 299
- hiding Burn Disc command 301
- hiding Chooser and Network Browser 293
- hiding disk and server icons 297
- hiding Eject command 300
- hiding Restart and Shut Down buttons on login 306
- hiding Restart and Shut Down commands 301
- hiding Trash warning 298
- importing users and groups in 179
- managing Classic sleep 294
- managing computer preferences 286
- managing email preferences 304
- managing group preferences 286
- managing user preferences 285
- managing Web preferences 304
- moving computers between accounts 275
- opening applications on login 307
- opening without authenticating 59
- populating Active Directory domains with 105
- populating LDAPv3 domains with 103
- presets 273
- preventing access to control panels 292
- refreshing account lists 175
- removing share points 216
- removing users from groups 168
- resharing NFS mounts in AFP 215
- restricting access to printers 314
- restricting changes to printer list 312
- restricting direct-connect printing 312
- restricting hard disk access 310
- searching for computer accounts 276
- setting default and computer views 303
- setting default printer 313
- setting desktop view 302
- setting Dock appearance 294
- setting Finder window display 297
- setting preferences 60
- setting up Guest Computers account 277
- setting up login window 305
- setting up share points 211, 213
- shortcuts 176
- showing Apple menu items 293
- showing file extensions 298
- showing password hint 306
- solving problems 202
- sorting account lists 175
- specifying a Classic System Folder 291
- starting Classic at login 291
- stopping sharing an item 216
- system preferences and 281
- task summary 60
- updating managed preference cache 283
- viewing access privileges for share points 217
- viewing read-only group accounts 167
- viewing read-only user accounts 139
- viewing share points 217
- workgroups
 - See also* Macintosh Manager

- about 128
- defined 590
- Mac OS 9 and 8 436
- planning 136
- World privileges for NFS 210
- World Wide Web Server predefined account 130
- Write Only privileges 205
- www (predefined group account) 132

X

- Xserve 487

