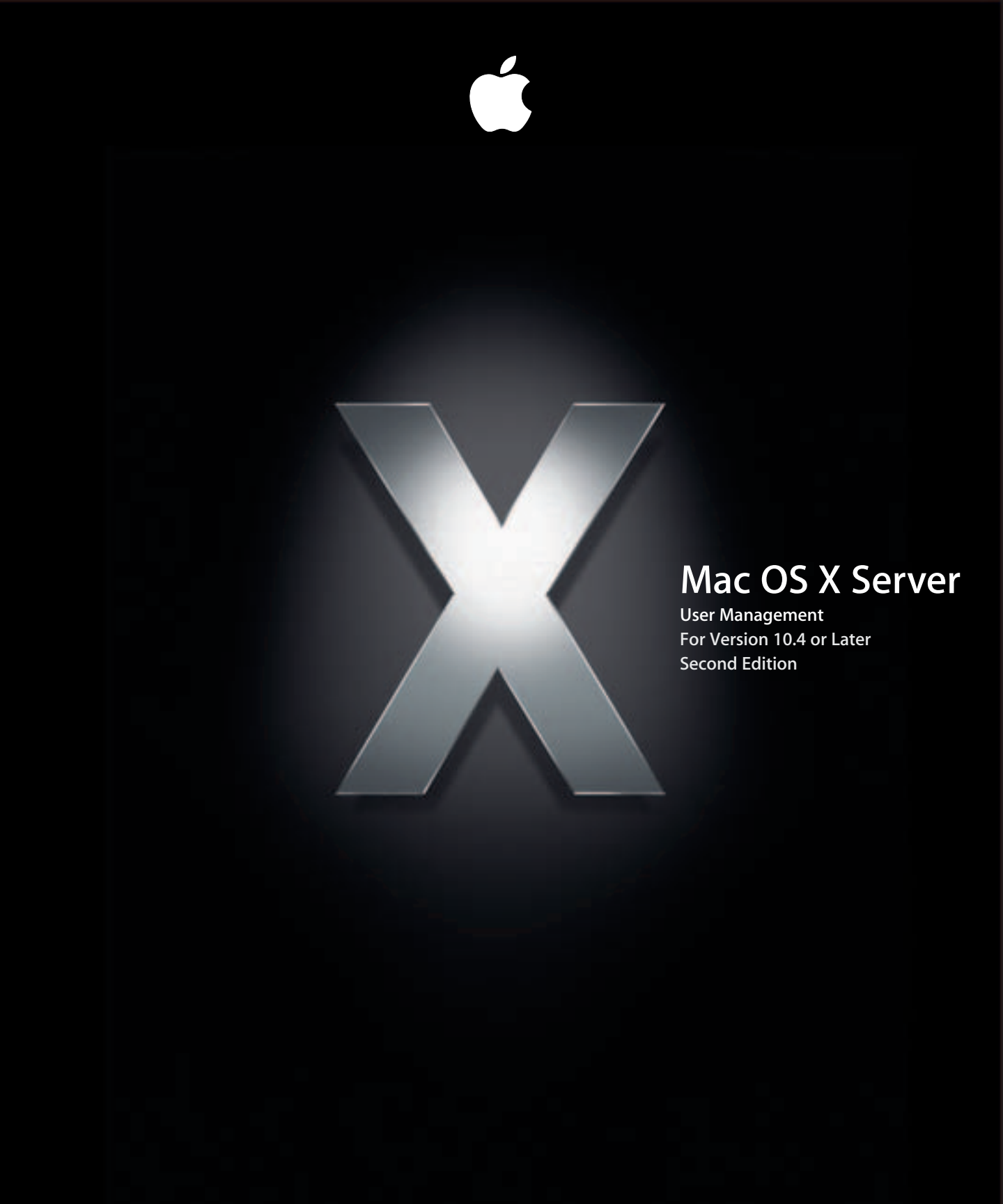


Mac OS X Server

User Management
For Version 10.4 or Later
Second Edition

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

019-0638/02-14-06

Contents

Preface 13 **About This Guide**
13 What's New in Version 10.4
14 What's in This Guide
15 Using Onscreen Help
16 The Mac OS X Server Suite
17 Getting Additional Information

Chapter 1 19 **User Management Overview**
19 Tools for User Management
19 Workgroup Manager
20 Server Admin
21 NetBoot
21 Network Install
22 Accounts
22 Administrator Accounts
23 User Accounts
24 Group Accounts
25 Computer Lists
25 The User Experience
26 Authentication and Identity Validation
27 Information Access Control

Chapter 2 29 **Getting Started with User Management**
29 Setup Overview
33 Planning Strategies for User Management
33 Analyzing Your Environment
33 Identifying Directory Services Requirements
34 Determining Server and Storage Requirements
35 Using Client Management
35 Choosing a Home Folder Structure
36 Devising a Home Folder Distribution Strategy
36 Identifying Groups
37 Determining Administrator Requirements

Chapter 3 39 **Getting Started with Workgroup Manager**
39 Configuring the Administrator's Computer and Account
40 Setting Up an Administrator Computer
40 Creating a Domain Administrator Account
41 Using Workgroup Manager
41 Working with Pre–Version 10.4 Computers from Version 10.4 Servers
41 Connecting and Authenticating to Directory Domains in Workgroup Manager
42 Major Workgroup Manager Tasks
43 Listing and Finding Accounts
43 Working with Account Lists in Workgroup Manager
44 Listing Accounts in the Local Directory Domain
44 Listing Accounts in Search Policy Directory Domains
45 Listing Accounts in Available Directory Domains
45 Refreshing Account Lists
46 Finding Specific Accounts in a List
46 Sorting User and Group Lists
46 Using the Search Button in the Toolbar
47 Shortcuts for Working with Accounts
47 Editing Multiple Accounts Simultaneously
47 Using Presets
48 Importing and Exporting Account Information
48 Backing Up and Restoring User Management Data
48 Backing Up and Restoring Directory Domain and Authentication Files
48 Backing Up Root and Administrator User Accounts

Chapter 4 49 **Setting Up User Accounts**
49 About User Accounts
49 Where User Accounts Are Stored
50 Predefined User Accounts
51 Administering User Accounts
51 Creating Mac OS X Server User Accounts
52 Editing User Account Information
52 Editing Multiple User Accounts Simultaneously
53 Modifying Accounts in an Open Directory Master
53 Working with Read-Only User Accounts
54 Working with Guest Users
54 Deleting a User Account
54 Disabling a User Account
54 Working with Presets
55 Creating a Preset for User Accounts
55 Using Presets to Create New Accounts
56 Renaming Presets
56 Editing Presets

56 Deleting a Preset
57 Working with Basic Settings
57 Defining User Names
58 Defining Short Names
59 Choosing Stable Short Names
59 Avoiding Duplicate Names
60 Defining User IDs
61 Defining Passwords
61 Setting Password Options for Imported User Accounts
62 Assigning Administrator Privileges for a Server
62 Assigning Administrator Privileges for a Directory Domain
63 Working with Advanced Settings
63 Defining Login Settings
64 Choosing a Password Type and Setting Password Options
65 Creating a Master List of Keywords
66 Applying Keywords to User Accounts
66 Editing Comments
67 Working with Group Settings
67 Defining a User's Primary Group
68 Adding a User to Groups
68 Removing a User from a Group
69 Reviewing a User's Group Memberships
69 Working with Home Settings
69 Working with Mail Settings
70 Enabling Mail Service Account Options
71 Disabling a User's Mail Service
71 Forwarding a User's Mail
72 Working with Print Settings
72 Enabling a User's Access to Print Queues that Enforce Quotas
73 Disabling a User's Access to Print Queues that Enforce Quotas
73 Deleting a User's Print Quota for a Specific Queue
73 Resetting a User's Print Quota
74 Working with Info Settings
75 Choosing Settings for Windows Users

Chapter 5 77 **Setting Up Group Accounts**
77 About Group Accounts
78 Where Group Accounts Are Stored
78 Predefined Group Accounts
79 Administering Group Accounts
79 Creating Mac OS X Server Group Accounts
80 Creating a Preset for Group Accounts
80 Editing Group Account Information

81 Creating Nested Groups
81 Upgrading Legacy Groups
82 Working with Read-Only Group Accounts
82 Deleting a Group Account
83 Working with Member Settings for Groups
83 Adding Users to a Group
84 Removing Users from a Group
84 Naming a Group
85 Defining a Group ID
86 Working with Group Folder Settings
86 Specifying No Group Folder
86 Creating a Group Folder
88 Designating a Group Folder for Use by Multiple Groups

Chapter 6 89 **Setting Up Computer Lists**
89 About Computer Lists
90 Special Purpose Computer Lists
91 Working with Guest Computers
92 Administering Computer Lists
92 Creating a Computer List
93 Creating a Preset for Computer Lists
93 Using a Computer List Preset
94 Adding Computers to an Existing Computer List
95 Changing Information About a Computer
95 Moving a Computer to a Different Computer List
95 Removing Computers from a Computer List
96 Deleting a Computer List
96 Searching for Computer Lists
97 Working with Access Settings
97 Restricting Access to Computers
98 Making Computers Available to All Users
98 Using Local User Accounts

Chapter 7 101 **Setting Up Home Folders**
101 About Home Folders
102 Hosting Home Folders for Mac OS X Clients
103 Hosting Home Folders for Other Clients
103 Distributing Home Folders Across Multiple Servers
104 Administering Share Points
104 Setting Up a Local Share Point
105 Setting Up an Automountable AFP Share Point for Home Folders
106 Setting Up an Automountable NFS Share Point for Home Folders
107 Administering Home Folders

107 Specifying No Home Folder
108 Creating a Home Folder for a Local User
109 Creating a Network Home Folder
110 Creating a Custom Location for Home Folders
113 Setting Disk Quotas
113 Choosing Default Home Folders by Using Presets
113 Moving Home Folders
113 Deleting Home Folders

Chapter 8 115 **User Management for Portable Computers**
115 About Mobile Accounts
116 About Portable Home Directories
116 Logging In to Mobile Accounts
117 Considerations and Strategies for Deploying Mobile Accounts
117 Advantages of Using Mobile Accounts
119 Disadvantages of Using Mobile Accounts
120 Strategies for Synchronizing Content
121 Setting Up Mobile Accounts for Use on Portable Computers
121 Configuring Portable Computers
122 Managing Mobile Clients Without Using Mobile Accounts
122 Unknown Mac OS X Portable Computers
123 Using Mac OS X Portable Computers with One Primary Local User
123 Using Max OS X Portable Computers with Multiple Local Accounts
124 Security Considerations for Mobile Clients
125 Preventing Unauthorized Computer Access
126 Directory Services
126 FileVault for Mobile Clients

Chapter 9 127 **Client Management Overview**
128 Using Network-Visible Resources
129 Customizing the User Experience
130 The Power of Preferences
131 Designing the Login Experience
134 Improving Workflow
135 Using Images to Install Software and Start Up Computers
136 Day-to-Day Computer Administration

Chapter 10 137 **Managing Preferences**
138 How Workgroup Manager Works with Mac OS X Preferences
139 Understanding Managed Preference Interaction
141 Setting the Permanence of Management
142 Caching Preferences
143 Managing Preferences

143 About the Preferences Cache
144 Updating the Managed Preferences Cache at Intervals
144 Updating the Preference Cache Manually
145 Managing User Preferences
145 Managing Group Preferences
146 Managing Computer Preferences
147 Editing Preferences for Multiple Records
147 Disabling Management for Specific Preferences
148 Managing Access to Applications
148 Creating a List of Applications Users Can Open
149 Preventing Users from Opening Applications on Local Volumes
149 Managing Access to Helper Applications
150 Controlling the Operation of UNIX Tools
151 Managing Classic Preferences
152 Selecting Classic Startup Options
152 Choosing a Classic System Folder
153 Allowing Special Actions During Restart
154 Controlling Access to Classic Apple Menu Items
155 Adjusting Classic Sleep Settings
155 Maintaining Consistent User Preferences for Classic
156 Managing Dock Preferences
157 Controlling the User's Dock
157 Providing Easy Access to Group Folders
158 Adding Items to a User's Dock
159 Preventing Users from Adding or Deleting Items in the Dock
160 Managing Energy Saver Preferences
160 Using Sleep and Wake Settings for Desktop Computers
161 Working with Energy Saver Settings for Portable Computers
163 Displaying Battery Status for Users
163 Scheduling Automatic Startup, Shutdown, or Sleep
164 Managing Finder Preferences
165 Setting Up Simple Finder
166 Keeping Disks and Servers from Appearing on the User's Desktop
166 Controlling the Behavior of Finder Windows
167 Hiding the Alert Message When a User Empties the Trash
167 Making Filename Extensions Visible
168 Controlling User Access to Remote Servers
168 Controlling User Access to an iDisk
168 Preventing Users from Ejecting Disks
169 Hiding the Burn Disc Command in the Finder
169 Controlling User Access to Folders
170 Removing Restart and Shut Down from the Apple Menu
170 Adjusting the Appearance and Arrangement of Desktop Items

171 Adjusting the Appearance of Finder Window Contents
172 Managing Internet Preferences
173 Setting Email Preferences
173 Setting Web Browser Preferences
174 Managing Login Preferences
175 Specifying How a User Logs In
176 Opening Items Automatically After a User Logs In
177 Providing Access to a User's Network Home Folder
177 Providing Easy Access to the Group Share Point
178 Preventing Restarting or Shutting Down the Computer at Login
179 Using Hints to Help Users Remember Passwords
179 Enabling Multiple Simultaneous Users on a Client Computer
180 Enabling Automatic Logout for Idle Users
181 Enabling the Use of Login and Logout Scripts
182 Running a Login or Logout Script
183 Managing Media Access Preferences
184 Controlling Access to CDs, DVDs, and Recordable Discs
184 Controlling Access to Hard Drives and Disks
185 Ejecting Items Automatically When a User Logs Out
186 Managing Mobility Preferences
186 Creating a Mobile Account
187 Preventing the Creation of a Mobile Account
188 Removing Mobile Accounts from Client Computers
189 Choosing Folders to Synchronize at Login and Logout, or in the Background
190 Setting the Background Synchronization Frequency
191 Managing Network Preferences
191 Configuring Proxy Servers by Port
192 Allowing Users to Bypass Proxy Servers for Specific Domains
193 Managing Printing Preferences
193 Making Printers Available to Users
194 Preventing Users from Modifying the Printer List
194 Restricting Access to Printers Connected to a Computer
195 Setting a Default Printer
195 Restricting Access to Printers
196 Managing Software Update Preferences
197 Managing Access to System Preferences
198 Managing Universal Access Preferences
199 Adjusting the User's Display Settings
200 Setting a Visual Alert
200 Adjusting Keyboard Responsiveness
201 Adjusting Mouse and Pointer Responsiveness
202 Enabling Universal Access Shortcuts
202 Allowing Devices for Users with Special Needs

203 Using the Preference Editor with Preference Manifests
204 Adding an Application to the Preference Editor's Application List
204 Editing an Application's Preferences with the Preference Editor
206 Disabling Management of an Application's Preferences Using the Preference Editor

Chapter 11 207 **Managing Network Views**
208 About Network Views
208 Types of Network Views
209 Administering Network Views
209 Creating a Network View
210 Renaming a Network View
211 Deleting a Network View
211 Enabling or Disabling a Network View
211 Adding Neighborhoods to Network Views
212 Deleting Neighborhoods from Network Views
212 Adding Computers to Network Views
214 Editing Computers in Network Views
214 Deleting Computers from Network Views
215 Adding Dynamic Lists to Network Views
215 Deleting Dynamic Lists from Network Views
216 Working with Network Views on Client Computers
216 How a Computer Finds Its Network Views
217 Naming a Network View to Associate It with a Computer
217 Adding Network View Clients
218 Removing Client Computers from Network Views
219 Disabling Network View Visibility for Specific Computers
219 Setting the Network View Update Rate
220 Setting Finder Behavior with Network Views

Chapter 12 221 **Solving Problems**
221 Diagnosing Common Network Issues
221 Testing Your Network's Time and Time Zones
222 Testing Your DNS Service
223 Testing Your DHCP Service
224 Solving Account Problems
224 You Can't Modify an Account Using Workgroup Manager
224 Users Can't See Their Names in the Login Window
224 You Can't Unlock an LDAP Directory
224 You Can't Modify a User's Open Directory Password
225 You Can't Change a User's Password Type to Open Directory
225 You Can't Assign Server Administrator Privileges
225 Users Can't Log In or Authenticate
226 Users Relying on a Password Server Can't Log In

226 Users Can't Log In with Accounts in a Shared Directory Domain
227 Users Can't Access Their Home Folders
227 Users Can't Change Their Passwords
227 Users Can't Authenticate Using Single Sign-On or Kerberos
227 Solving Preference Management Problems
227 You Can't Enforce Default Web Settings
227 You Can't Enforce Default Mail Settings
228 Users Don't See a List of Workgroups at Login
228 Users Can't Open Files
228 Users Can't Add Printers to a Printer List
229 Login Items Added by a User Don't Open
229 Items Placed in the Dock by a User Are Missing
229 A User's Dock Has Duplicate Items
230 Users See a Question Mark in the Dock
230 Users See a Message About an Unexpected Error

Appendix A 231 **Importing and Exporting Account Information**
231 Understanding What You Can Import and Export
232 Limitations for Importing and Exporting Passwords
232 Archiving the Open Directory Master
232 Using Workgroup Manager to Import Users and Groups
233 Using Workgroup Manager to Export Users and Groups
234 Using dsimport to Import Users and Groups
234 Using XML Files Created with Mac OS X Server Version 10.1 or Earlier
235 Using XML Files Created with AppleShare IP 6.3
236 Using Character-Delimited Files
236 Writing a Record Description

Appendix B 239 **ACL Permissions and Group Memberships Using GUIDs**
239 Understanding GUIDs
240 GUIDs and File Permissions
240 ACLs and POSIX Permissions
241 File Permissions and Synchronization
241 SIDs and Windows Interoperability
241 GUIDs and Group Memberships
241 Importing and Exporting GUIDs
242 Maintaining GUIDs When Importing from Earlier Versions of Mac OS X Server
242 Using GUIDs When Importing and Exporting Users
243 Working with GUIDs
243 Viewing GUIDs

Glossary 245

Index 253

About This Guide

This guide explains how to use Workgroup Manager to set up and manage home folders, accounts, preferences, and settings for clients.

Mac OS X Server includes Workgroup Manager, a user management tool you can use to create and manage accounts, share points, and network views. When managing accounts, you can define core account settings like name, password, home folder location, and group membership. You can also manage preferences, allowing you to customize the user's experience, granting or restricting access to his or her own computer's settings and to network resources.

Workgroup Manager works closely with a directory domain. Directory domains are like databases, only specifically geared towards storing account information and handling authentication.

What's New in Version 10.4

- **Portable home directories**. Users with portable computers can now have portable home directories, which synchronize local and network home folders. Synchronization updates the portable home directory based on which folder contains the most recently modified files. For more information, see "About Portable Home Directories" on page 116.
- **Managed network views.** You can now control what users see when they select the Network icon in the sidebar of a Finder window (or choose Go > Network). A managed network view can contain one or more neighborhoods, which appear in the Finder as folders. Each folder contains a list of resources, like networked computers or dynamic lists. Managed network views offer a meaningful way to present network resources. You can create different views for different client computers. And because Open Directory stores the views, a computer's neighborhood is automatically available when a user logs in. For more information, see Chapter 11, "Managing Network Views," on page 207.

- **Preference manifests and preference editor.** If you want fine-grained control of preference settings, you can work with Workgroup Manager's new preference editor, which can use preference manifests. Preference manifests are files that describe the structure and values of an application's preferences. The preference editor can create or edit any property list (plist) and incorporates preference manifests to thoroughly describe preference settings that customize the behavior of applications and utilities. For more information, see "Using the Preference Editor with Preference Manifests" on page 203.
- **User information.** You can enter and edit personal data for each user, such as addresses, phone numbers, iChat names, and webpage URLs. The Address Book application can access this information. For more information, see "Working with Info Settings" on page 74.

What's in This Guide

This guide is organized as follows:

- Chapter 1, "User Management Overview," highlights important concepts, introduces the user management tools, and tells you where to find additional information about user management and related topics.
- Chapter 2, "Getting Started with User Management," describes how to use features and shortcuts to maximize efficiency when setting up and maintaining accounts and managed preferences.
- Chapter 3, "Getting Started with Workgroup Manager," describes how to set up Workgroup Manager and use its core features.
- Chapters 4, 5, and 6 tell you how to use Workgroup Manager to set up users, groups, and computer lists.
- Chapter 7, "Setting Up Home Folders," covers creating home folders.
- Chapter 8, "User Management for Portable Computers," discusses considerations for managing portable computers.
- Chapter 9, "Client Management Overview," introduces client management tools and concepts, such as how to customize a user's working environment and provide user access to network resources.
- Chapter 10, "Managing Preferences," describes how to use Workgroup Manager to control preference settings for users, groups, and computers that use Mac OS X.
- Chapter 11, "Managing Network Views," discusses how you can create network views in Workgroup Manager to customize the browsing experience for each computer and control what appears in the Network folder in the Finder of that computer.
- Chapter 12, "Solving Problems," helps you address issues involving account creation, home folder maintenance, preference management, or client setup; and also helps you solve problems encountered by managed clients.

- Appendix A, "Importing and Exporting Account Information," provides information you'll need when you want to transfer account information to or from an external file.
- Appendix B, "ACL Permissions and Group Memberships Using GUIDs," describes a new user identifier introduced in Mac OS X version 10.4.
- The Glossary defines terms you'll encounter as you read this guide.

Note: Because Apple frequently releases new versions and updates to its software, images shown in this book may be different from what you see on your screen.

Using Onscreen Help

If you want to work with accounts, change preference settings, set up new home folders, or do any other day-to-day administration task, you can find step-by-step procedures by using the onscreen help available in Workgroup Manager. While all the administration tasks are also documented in this guide, sometimes it's more convenient to retrieve information in onscreen help while working online.

On a computer running Mac OS X Server, you can access onscreen help after opening Workgroup Manager or Server Admin. From the Help menu, choose one of these options:

- *Workgroup Manager Help* or *Server Admin Help* displays information about the application.
- *Mac OS X Server Help* displays the main server help page, from which you can search or browse for server information.
- *Documentation* takes you to www.apple.com/server/documentation/, where you can download server documentation.

You can also access onscreen help from the Finder, or from other applications on a server or administrator computer. (An administrator computer is any Mac OS X computer with server administration software installed on it.) Use the Help menu to open Help Viewer, and then choose Library > Mac OS X Server Help.

To see the latest server help topics, make sure the server or administrator computer is connected to the Internet while you're using Help Viewer. Help Viewer automatically retrieves and caches the latest server help topics from the Internet. When your computer is not connected to the Internet, Help Viewer displays cached help topics.

The Mac OS X Server Suite

The Mac OS X Server documentation includes a suite of guides that explain the available services and provide instructions for configuring, managing, and troubleshooting these services. All of the guides are available in PDF format from:

www.apple.com/server/documentation/

This guide ...	tells you how to:
Mac OS X Server Getting Started for Version 10.4 or Later	Install Mac OS X Server and set it up for the first time.
Mac OS X Server Upgrading and Migrating to Version 10.4 or Later	Use data and service settings that are currently being used on earlier versions of the server.
Mac OS X Server User Management for Version 10.4 or Later	Create and manage users, groups, and computer lists. Set up managed preferences for Mac OS X clients.
Mac OS X Server File Services Administration for Version 10.4 or Later	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB/CIFS.
Mac OS X Server Print Service Administration for Version 10.4 or Later	Host shared printers and manage their associated queues and print jobs.
Mac OS X Server System Image and Software Update Administration for Version 10.4 or Later	Use NetBoot and Network Install to create disk images from which Macintosh computers can start up over the network. Set up a software update server for updating client computers over the network.
Mac OS X Server Mail Service Administration for Version 10.4 or Later	Set up, configure, and administer mail services on the server.
Mac OS X Server Web Technologies Administration for Version 10.4 or Later	Set up and manage a web server, including WebDAV, WebMail, and web modules.
Mac OS X Server Network Services Administration for Version 10.4 or Later	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.
Mac OS X Server Open Directory Administration for Version 10.4 or Later	Manage directory and authentication services.
Mac OS X Server QuickTime Streaming Server Administration for Version 10.4 or Later	Set up and manage QuickTime streaming services.
Mac OS X Server Windows Services Administration for Version 10.4 or Later	Set up and manage services including PDC, BDC, file, and print for Windows computer users.
Mac OS X Server Migrating from Windows NT for Version 10.4 or Later	Move accounts, shared folders, and services from Windows NT servers to Mac OS X Server.

This guide ...	tells you how to:
Mac OS X Server Command-Line Administration for Version 10.4 or Later	Use commands and configuration files to perform server administration tasks in a UNIX command shell.
Mac OS X Server Collaboration Services Administration for Version 10.4 or Later	Set up and manage weblog, iChat, and other services that facilitate interactions among users.
Mac OS X Server High Availability Administration for Version 10.4 or Later	Manage IP failover, link aggregation, load balancing, and other hardware and software configurations to ensure high availability of Mac OS X Server services.
Mac OS X Server Xgrid Administration for Version 10.4 or Later	Manage computational Xserve clusters using the Xgrid application.
Mac OS X Server Glossary: Includes Terminology for Mac OS X Server, Xserve, Xserve RAID, and Xsan	Interpret terms used for server and storage products.

Getting Additional Information

For more information, consult these resources:

Mac OS X Server website (www.apple.com/server/macosx/)—gateway to extensive product and technology information.

AppleCare Knowledge Base (kbase.info.apple.com)—access to hundreds of articles from Apple's support organization.

Apple customer training (train.apple.com)—instructor-led and self-paced courses for honing your server administration skills.

Apple discussion groups (discussions.info.apple.com)—a way to share questions, knowledge, and advice with other administrators.

Apple mailing list directory (www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using email.

Read Me documents—important updates and special information. Look for them on the server discs.

User Management Overview

1

This chapter introduces user management concepts and describes the applications you'll use to manage accounts and privileges.

User management encompasses everything from setting up accounts for network access and creating home folders, to fine-tuning the user experience by managing preferences and settings for users, groups, and computer lists. Mac OS X Server provides tools for accomplishing these tasks and more.

Tools for User Management

User management tools and technologies in Mac OS X Server include Workgroup Manager, Server Admin, NetBoot, and Network Install.

Workgroup Manager

Workgroup Manager is a powerful tool that delivers features for comprehensive management of Macintosh clients. You can use Workgroup Manager on a Mac OS X Server computer, or you can install and use Workgroup Manager on a Mac OS X computer.

Workgroup Manager provides a centralized method of managing Mac OS X computers, controlling access to software and removable media, and providing a consistent, personalized experience for users at different levels, whether they're beginners in a classroom or advanced users in an office.

You'll use Workgroup Manager to create user accounts and set up groups to provide convenient access to resources. You can add and configure computer lists, which can selectively permit or deny privileges to users or groups for specific computers or printers. You can manage user settings for mail, printing, and home folders. Workgroup Manager allows you to configure and manage share points, which host home folders. You can also use account settings and managed preferences to achieve the level of administrative control you need, as well as establishing the most efficient user experience.

By using Workgroup Manager with Mac OS X Server services, you can:

- Customize the working environments of network users, by organizing their desktop resources and personal files.
- Enable services that require user accounts, such as mail, file sharing, iChat service, and Weblog service.
- Share system resources such as printers and computers, maximizing their availability and making sure that disk space and printer usage remain equitably shared.

This guide provides instructions for user management tasks that you can complete with Workgroup Manager. To get started with Workgroup Manager, see Chapter 3, "Getting Started with Workgroup Manager," on page 39.

Server Admin

The Server Admin application provides access to various tools and services that play a role in server management. Once you have installed the Mac OS X Server software, set up directory services, and established your network, you can user Workgroup Manager to start creating and managing accounts. After setting up accounts and home folders, you can use Server Admin to set up additional services to provide mail service, host websites or share printers. Workgroup Manager can then be used to create share points, allowing users to share folders and files.

For instructions on completing tasks using the many services managed through Server Admin, see the service administration guides. The following table lists common server administration tasks, and includes where to find related documentation.

If you want to	See this document
Assign permissions to folders and files within a share point	Mac OS X Server File Services Administration For Version 10.4 or Later
Share printers among users	Mac OS X Server Print Service Administration For Version 10.4 or Later
Set up websites or WebDAV support on the server	Mac OS X Server Web Technologies Administration For Version 10.4 or Later
Provide email service for users	Mac OS X Server Mail Service Administration For Version 10.4 or Later
Broadcast multimedia in real time from the server	Mac OS X Server QuickTime Streaming Server Administration For Version 10.4 or Later
Provide identical operating system and applications folders for client computers	Mac OS X Server System Image and Software Update Administration for Version 10.4 or Later
Install applications across a network	Mac OS X Server System Image and Software Update Administration for Version 10.4 or Later
Share information among multiple Mac OS X Server systems or Mac OS X computers	Mac OS X Server Open Directory Administration For Version 10.4 or Later

For a complete list of Mac OS X Server documentation, see “The Mac OS X Server Suite” on page 16.

NetBoot

Mac OS X computers can start up from a network-based NetBoot image, providing quick and easy configuration of department, classroom, and individual systems, as well as web and application servers, throughout a network. When you update a NetBoot image, all computers using NetBoot have instant access to the new configuration. You can set up multiple NetBoot images, to customize the computer setup for different groups of clients.

NetBoot can simplify administration and reduce the support normally associated with large-scale deployments of network-based Macintosh computers. NetBoot is ideal for an organization with 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.

With NetBoot, you can quickly configure and update client computers by updating a NetBoot image stored on the server. NetBoot images contain 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 restart. Systems that are compromised or otherwise altered can be instantly restored by restarting them.

You use System Image Utility to create and modify NetBoot images and use NetBoot to deploy NetBoot images.

For more information about these tools or about installing an operating system over a network, see the system image and software update administration guide.

Network Install

Network Install is a centralized software installation service. It lets you selectively and automatically install, restore, or upgrade network-based Macintosh systems anywhere in your organization. Installation images can contain the latest version of Mac OS X, a software update, site-licensed or custom applications, or configuration scripts.

You can use Network Install to upgrade operating systems, install software updates and custom software packages, or reimage desktop and portable computers. You can define custom installation packages for various departments in an organization, such as marketing, engineering, and sales.

With Network Install you don’t need to use CDs or DVDs to configure a computer. All the installation files and packages reside on the server and are installed on the client computer together. With Network Install, you can run pre- and post-installation scripts to perform system commands before or after the installation of a software package or system image.

You use System Image Utility or PackageMaker to create Network Install packages, and you use NetBoot to deploy Network Install packages.

For more information about using these tools with Network Install, see the system imaging and software update administration guide.

Accounts

In order to use Workgroup Manager to manage accounts, you use an administrator account. With an administrator account, you can set up and manage three types of accounts using Workgroup Manager: user accounts, group accounts, and computer lists.

When you define a user account, you specify the information needed to prove the user's identity: user name, and password. You can also specify a user identification number (user ID), which is useful for folder and file permissions. 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. In addition to the accounts you create, Mac OS X Server has some predefined user and group accounts, some of which are reserved for use by Mac OS X.

Administrator Accounts

Users with server or directory domain administration privileges are known as *administrators*. An administrator can be a server administrator, domain administrator, or both. Server administrator privileges determine whether a user can view information about or change the settings of a particular server. Domain administrator privileges determine the extent to which the administrator can view or change the account settings for users, groups, and computer lists in the directory domain.

Server Administration

Server administration privileges determine the powers a user has when logged in to a particular Mac OS X Server. For example, a server administrator can use Server Admin and can make changes to a server's search policy using Directory Access.

When you assign server administration privileges to a user, the user is added to the predefined group named "admin" in the local directory domain of the server. Many Mac OS X applications—such as Server Admin, Directory Access, and System Preferences—use the admin group to determine whether a particular user can perform certain administrative activities with the application. The primary administrator defined when using Server Assistant is user ID 501 in the server's local directory domain.

Local Mac OS X Computer Administration

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

Directory Domain Administration

In Mac OS X Server, when you create a directory domain, a domain administrator account is also created and added to the admin group in the domain. The user ID of the domain administrator defaults to 1000 when the account creation dialogue appears, at which time you also have to set the name and password. The domain administrator account is also a server administrator account, but the server administrator is not a domain administrator by default. Each directory domain has its own domain administrator account, and a domain administrator can create additional domain administrators in the same domain.

You can allow certain users to manage specific accounts. 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 a directory domain administrator (an administrator of that domain).

You can control the extent to which a directory domain administrator can use Workgroup Manager to change account data stored in a domain. For example, you may want to set up directory domain privileges so your network administrator can add and remove user accounts, but other users can change the information for particular users. Or you may want to designate multiple administrators 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.

For more information about how to set up a directory domain administrator account, see "Creating a Domain Administrator Account" on page 40.

User Accounts

Depending on how you set up your server and your user accounts, you can use Mac OS X Server to support users who log in using Mac OS X computers, Windows computers, or UNIX computers.

Most users have an individual account used to authenticate them and control their access to services. When you want to personalize a user's environment, you define user, group, or computer preferences for that user. The term *managed client* or *managed user* designates a user who has administrator-controlled preferences associated with his or her account. *Managed client* is also used to refer to computer lists that have preferences defined for them.

When a managed user logs in, the preferences that take effect are a combination of the user's preferences and the preferences set up for any workgroup or computer list the user belongs to.

To learn more about how to set up user accounts, see Chapter 4, "Setting Up User Accounts." To specify the preferences for user accounts, see Chapter 10, "Managing Preferences."

Guest Users

You may 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*.

With some services, such as AFP, you can specify whether to let guest users access files. If you enable guest access, users who connect anonymously are restricted to files and folders with permissions set to Everyone. Instead of authenticating with a name and a password, a guest user connects as a guest, not as a registered user.

Group Accounts

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 permission to access certain files or folders on a volume.

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

Information in group accounts helps control user access to folders and files. See "Folder and File Access by Other Users" on page 28 for a description of how this works.

Groups can be nested within groups. For example, a group can be a member of another group. A group that contains another group is called a *parent group*, and the group that is contained is called a *nested group*. Nested groups are useful for inheriting access permissions, but they do not inherit managed preferences.

To learn more about how to set up group accounts, see Chapter 5, "Setting Up Group Accounts." To specify preferences for group accounts, see Chapter 10, "Managing Preferences."

Workgroups

When you define preferences for a group, it is known as a *workgroup*. A workgroup lets you manage the working environment of group members.

Any preferences you define for a Mac OS X workgroup are stored in the group account. See Chapter 10, "Managing Preferences," on page 137 for a description of workgroup preferences.

Group Folders

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

You can give individual users permission to write to a group folder, or to change group folder attributes in the Finder.

Computer Lists

A computer list is composed of one or more computers that have the same managed preferences and that are available to particular users and groups. You can create and modify computer lists in Workgroup Manager.

To learn more about how to set up computer lists for Mac OS X client computers, see Chapter 6, "Setting Up Computer Lists." To specify preferences for Mac OS X computer lists, see Chapter 10, "Managing Preferences."

Guest Computers

Most computers on your network should be in a named computer list. If an unknown computer (one that isn't already in a computer list) connects to your network and attempts to access services, that computer is treated as a *guest*. Settings chosen for a Guest Computers list apply to these unknown guest computers.

The User Experience

Once you have created an account for a user, the user can access server resources according to the permissions you have set. For most users, the typical flow of events from login to logout occurs as follows:

- **Authentication**. The user enters a name and password.
- **Identity validation**. The user name and password are verified by directory services.
- **Login**. The user can be granted access to the server and network resources.
- **Access**. The user connects to and uses approved servers, share points, and applications.
- **Logout**. The user's session is terminated.

Details of the user experience may vary depending upon the type of user, the permissions set, the type of client computer (such as Windows or UNIX) currently in use, whether the user is a member of a group, and whether preference management has been implemented at the user, group, or computer level.

You'll find information about the Mac OS X user experience in Chapter 9, "Client Management Overview." Basic information about authentication, identity validation, and information access control is given in the sections that follow.

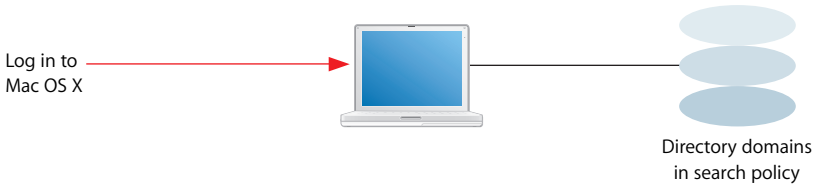
Authentication and Identity Validation

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

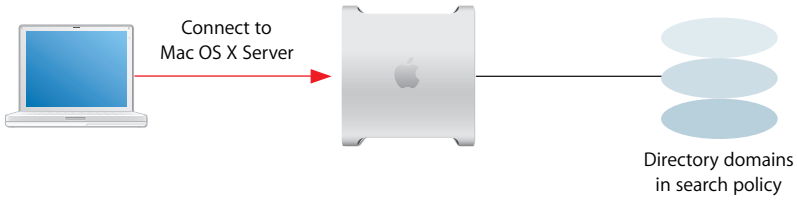
A Mac OS X computer can find user accounts that are stored in a directory domain of the computer's search policy.

- A *directory domain* stores information about users and resources. It 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.

The following picture shows a user logging in to a Mac OS X computer that can locate the user's account in a directory domain within its search policy.



After login, the user can connect to a remote server to gain access to its services, if the user's account can be located within the search policy of the server.



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 is validated, the user is authenticated and the login or connection process is completed.

Mac OS X Server can validate passwords using Kerberos, Open Directory Password Server, shadow passwords, and crypt passwords.

The Open Directory administration guide describes the different kinds of directory domains and tells you how to configure search policies on any Mac OS X computer. It also discusses different kinds of authentication methods and provides instructions for setting up user authentication options.

Information Access Control

Mac OS X version 10.4 uses globally unique identifiers (GUIDs) to keep track of folder and file permissions. GUIDs are 128-bit values, which makes duplicate GUIDs extremely unlikely.

Before Mac OS X version 10.4, Mac OS X exclusively used a particular data item in a user's account—the user ID—in conjunction with POSIX permissions to keep track of folder and file permissions. In Mac OS X, all folders or files include POSIX permissions for entities such as:

- the owner
- the group
- everyone else

Unlike using GUIDs, using POSIX permissions can cause file ownership and group membership issues when there are multiple users with the the same short name or user ID. The introduction of GUIDs does not change or remove POSIX permissions, and thus it does not affect interoperability of Mac OS X with legacy UNIX systems or other operating systems.

Globally Unique Identifiers

Starting with Mac OS X version 10.4, a universal ID called a globally unique identifier (GUID, pronounced GOO-id) provides user and group identity for access control list (ACL) permissions. An ACL is a list of access control entries (ACEs), each specifying the permissions to be granted or denied to a group or user, and how these permissions are propagated throughout a folder hierarchy. The GUID also associates a user with group and nested group memberships.

A discussion of GUIDs and their implications appears in Appendix B, "ACL Permissions and Group Memberships Using GUIDs."

Folder and File Owner Access

When a folder or file is created, the file system stores the user ID of the user who created it. By default, when a user with that user ID accesses the folder or file, he or she can read and write to it. Also, any process started by the creator can read and write to any files associated with the creator's user ID.

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

Folder and File Access by Other Users

The use of GUIDs in conjuction with ACLs can determine file access by users and groups. Also, the user ID, in conjunction with a group ID, is 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 the user's account. When a user accesses a folder or file and the user isn't the owner, the file system checks the file's group permissions.

- If the user's primary group ID matches the ID of the group associated with the file, the user inherits group permissions.
- If the user's primary group ID doesn't match the file's group ID, Mac OS X searches for the group account that has permission to access the file. Once found, all members of that group and of subsequent nested groups are given permission to that file.
- If neither of these cases applies, the user's access permissions default to the generic "everyone."

Getting Started with User Management

2

This chapter provides information for planning and setting up a user management environment.

In order to create an effective user management environment, you should carefully plan and strategize how you will deploy your network. When deploying your network, you should systematically and methodically set up your network resources.

Setup Overview

This section provides an overview of user management setup tasks, with the goal of understanding the sequence in which an administrator would create a managed environment. Not all steps are necessary in every case.

Step 1: Before you begin, do some planning

Analyze your users' needs to determine which directory service configuration and home folder setup would best suit them. See "Planning Strategies for User Management" on page 33.

Step 2: Set up the server infrastructure

Before deploying client computers, make sure one or more computers with Mac OS X Server installed are set up for hosting accounts and share points. New servers come with Mac OS X Server software preinstalled.

Set up the server so that it hosts or provides access to shared directory domains. Shared directory domains (also called *shared directories*) contain user, group, and computer information you want many computers to be able to access. Users whose accounts reside in a shared directory are referred to as *network users.*

There are different kinds of shared directories. You can use Workgroup Manager to add or modify accounts that reside in read/write directory domains such as the LDAP directory of an Open Directory master, or a NetInfo domain. For read-only directory domains such as LDAPv2, read-only LDAPv3, or BSD flat files, make sure they are configured to support Mac OS X Server and that they provide needed account data. You might have to add, modify, or reorganize information in a directory to make the directory compatible.

Mac OS X offers a variety of options for authenticating users (including Windows users) whose accounts are stored in directory domains on Mac OS X Server. In addition, Mac OS X can access accounts in existing directories on your network, such as a Windows server's Active Directory.

Use file services to make resources visible throughout the network so that users can access them from different computers. Key network-visible resources include network home folders, group folders, and other shared folders.

If some of your users use Windows computers, you can also configure the server to provide them with file services, domain login, and home folders.

There are several administration guides that describe these services in detail.

- For installation requirements and guidelines, see the getting started guide.
- For information about directory services and authentication, see the Open Directory administration guide.
- For information about how to set up file services, see the file services administration guide.
- For information about how to set up servers for managing Windows users, see the Windows services administration guide.

Step 3: Set up an administrator computer

Because servers are usually kept in a secure, locked location, administrators typically conduct user management tasks remotely from any Mac OS X computer running version 10.4 or later. Such a computer is referred to in this guide as the administrator computer.

Before you can use the administrator computer to create and manage accounts in a shared directory, you need a user account in the shared directory and you need to be a domain administrator. A domain administrator can use Workgroup Manager to add and change accounts that reside in the LDAP directory of an Open Directory master, a NetInfo domain, or another read/write directory domain.

For instructions on setting up an administrator computer and creating domain administrator accounts, see Chapter 3, "Getting Started with Workgroup Manager."

Step 4: Set up a home folder share point

Home folders for accounts stored in shared directories can reside in a network share point that the user's computer can access.

You can set up network home folders so they can be accessed using either AFP or NFS. You can also set up home folders for exclusive use by Windows users using SMB/CIFS:

- For instructions on setting up AFP or NFS share points for network home folders for Macintosh users, see Chapter 7, "Setting Up Home Folders."
- For information about setting up SMB/CIFS share points for Windows user home folders, see the Windows services administration guide.

Step 5: Create user accounts and home folders

You can use Workgroup Manager to create user accounts in directories that reside on Mac OS X Server or in some other read/write directory domains. Detailed instructions appear in various locations in this guide:

- For information about how to create Mac OS X user accounts, see Chapter 4, "Setting Up User Accounts."
- For information about how to create Mac OS X mobile user accounts, see Chapter 8, "User Management for Portable Computers."
- For information about home folders, see Chapter 7, "Setting Up Home Folders."

You can also create accounts on Mac OS X Server to manage Windows users and provide Windows domain login, roaming user profiles, home folders, file services, mail service, and so on. See the Windows services administration guide for instructions.

Step 6: Set up client computers

Mac OS X Server can support users of Mac OS X and Windows client computers.

For Mac OS X computers, configure the search policy of the computers so that they can locate shared directory domains. For instructions, see the Open Directory administration guide.

For setup instructions for mobile Mac OS X computers that use AirPort to communicate with Mac OS X Server, see *Designing AirPort Extreme Networks* (available at www.apple.com/airportextreme/).

You can join Windows workstations to the Mac OS X Server primary domain controller (PDC). This is similar to how you configure Windows workstations to join a Windows NT server's domain. For more information, see the Windows services administration guide.

If you have more than just a few Macintosh client computers to set up, consider using Network Install to create a system image that automates client computer setup. For instructions, see the system image and software update administration guide.

To prevent unauthorized access to client computers, you need to secure them against both local and network threats. For a brief description of how to secure computers, see "Security Considerations for Mobile Clients" on page 124.

Step 7: Define user account preferences

You manage the working environment of Macintosh users whose accounts reside in a shared domain by defining user account preferences. For information about Mac OS X user preferences, see Chapter 9, "Client Management Overview," and Chapter 10, "Managing Preferences."

Step 8: Create group accounts and group folders

Use Workgroup Manager to create group accounts in directories that reside on Mac OS X Server and in some other read/write directory domains. You can create group folders to distribute documents and organize applications for group members.

- For information about how to work with Mac OS X group accounts and group folders, see Chapter 5, "Setting Up Group Accounts."
- For information about how to add the group folder to the dock to make it more accessible to users, see Chapter 10, "Managing Preferences."

Step 9: Define group account preferences

You can manage the preferences for a group of Macintosh users. A group with managed preferences is referred to as a *workgroup*. For information about Mac OS X workgroups, see Chapter 9, "Client Management Overview," and Chapter 10, "Managing Preferences."

Step 10: Define computer lists and preferences

Use computer lists if you want to manage client Macintosh computers.

- For information about creating Mac OS X computer lists, see Chapter 6, "Setting Up Computer Lists." For information about computer list preferences, see Chapter 9, "Client Management Overview," and Chapter 10, "Managing Preferences."
- Every Windows computer supported by the Mac OS X Server primary domain controller must be part of the Windows Computers computer list. See the Windows services administration guide for details.

Step 11: Perform ongoing account maintenance

As users come and go and the requirements for your servers change, you'll update account information periodically.

- For information about how to use Workgroup Manager to display accounts, see Chapter 3, "Getting Started with Workgroup Manager."
- Information in Chapter 4 through Chapter 8 helps you do common tasks such as defining a guest account, disabling user accounts, adding and removing users from groups, and deleting accounts.
- For solutions to common problems, see Chapter 12, "Solving Problems."

Planning Strategies for User Management

Here are some planning activities to undertake before you start to implement user management.

Analyzing Your Environment

Your user management settings need to complement your particular environment, including:

- The size and distribution of your network
- The number of users who access your network
- The kind of computers users use (Mac OS X or Windows)
- How users use client computers
- Which computers are mobile computers
- Which users should have administrator privileges
- Which users should have access to particular computers
- What services and resources users need (such as mail, or access to data storage)
- How you might divide users into groups (for example, by class topic or job function)
- How you want to group sets of computers (such as all computers in a public lab)

Identifying Directory Services Requirements

Identify the directories in which you'll store user and group accounts and computer lists.

- If you have an Active Directory or LDAP server already set up, you might be able to take advantage of existing account records. See the Open Directory administration guide for details about accessing existing directories.
- If you have an earlier version of an Apple server, you might be able to migrate existing records. See the updating and migrating guide for available options.
- Set up Open Directory master and replicas to host LDAP directories to store other user accounts, group accounts, and computer lists on your network. See the Open Directory administration guide for instructions and for complete information about password handling options.

Note: If not all the domains have been finalized when you're ready to start adding user and group accounts, simply add the accounts to any directory 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. Exporting and importing account information does not retain passwords. For more information, see Appendix A, "Importing and Exporting Account Information."

Determining Server and Storage Requirements

These requirements vary with the number of users and computers:

- For fewer than 450 users and fewer than 150 computers, one server is adequate for account management and authentication, home folders, and group folders. This guideline assumes that you provide each user 1 GB of storage space and that you are using an Xserve computer. More storage can be provided using additional drive modules and by using RAID.
- For 450–1000 users and 150–450 computers, one server is required for account management and authentication. You'll need one home folder and group folder server for every 150 computers. Adjust the total amount of storage available on the server to account for the number of computers. For 150 computers, provide approximately 180 GB of storage. Consider installing additional storage to give yourself some room to expand.

  One server acts as the Open Directory master; this server can also host primary services such as DNS, DHCP, and web service as needed. Group folders are often shared among many computers at the same time. Avoid more than 150–300 concurrent connections to a group folder by establishing multiple workgroups and distributing users into more than one workgroup.
- For over 1000 users and over 450 computers, you'll need multiple servers for account management and authentication. In order to use multiple servers for account management and authentication, you'll use replication. For more information about replication, see the Open Directory administration guide. You'll also need one home folder and group folder server and 180 GB of storage for every 150 concurrently connected computers, if the users have network home folders.
- You will ideally have several servers to allocate network services across. Instead of one server acting as both the Open Directory master and the host for primary services, you could dedicate one server to being the Open Directory master and have another server provide DNS, DHCP, NTP, and firewall. You could also have a server host an Open Directory replica, which provides failover protection. If additional dedicated services are needed, explore using servers specifically for those tasks, such as QuickTime streaming or Software Update. By deploying services on dedicated servers, you can more easily isolate and troubleshoot issues with specific services. If a hardware failure occurs, it will disrupt only the one service and not the rest of the network.

  By hosting collaboration services such as mail, iChat, and weblog on your own servers, you can control access to these services. These services are unique in that they can be used to communicate on a private network. You can configure these services to allow communication only within the network.
- Do not use more than six automountable share points per server. You may need to create fewer share points with subfolders, to logically distribute users into home folder sets.

Using Client Management

Take advantage of Macintosh client management if you want to do any of the following:

- Provide users with a consistent, controlled interface while allowing them access to their files from any computer
- Use mobile accounts and portable home directories
- Reserve certain resources for specific groups or individuals
- Secure computer use in key areas, such as administrative offices, classrooms, or open labs

Determine the users, groups, and computers whose preferences you want to manage. See Chapter 9, "Client Management Overview," on page 127 and Chapter 10, "Managing Preferences," on page 137 for planning guidelines.

Choosing a Home Folder Structure

When deploying computers, one of the most crucial decisions you have is choosing how and where to host home folders. There are three types of home folders: a local home folder, a network home folder, and a portable home directory. These home folders are typically tied, respectively, to local, network, and mobile accounts.

Users with local accounts typically have local home folders. When users save files in local home folders, the files are stored locally. To save the files over the network, the users have to connect to the network and upload the file. Using local home folders gives you the least control over an individual user's managed preferences. It also is not inherently tied to a network account.

Users with network accounts typically have network home folders. When they save files in their network home folders, the files are stored on the server. Additionally, whenever users access their home folders, even for common tasks like caching webpages, users' computers have to retrieve these files from the server. Using network home folders gives you complete control over an individual user's managed preferences. When users are not connected to the network, they cannot access their accounts or home folders.

Users with mobile accounts have both local and network home folders, which combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders. You can configure which folders to synchronize and how frequently to synchronize them. Mobile accounts also cache authentication information and managed preferences. If you synchronize key folders, a user can work on and off the network and experience a seamless work environment. If you choose to not synchronize portable home directories, mobile accounts are very similar to local accounts, except that mobile accounts have managed preferences.

Note: If a user's mobile account is hosted in an Active Directory domain, the mobile account will not have a portable home directory. However, it will have a local home folder and a network home folder, and it will be able to cache authentication.

Mobile accounts are described in detail in Chapter 8, "User Management for Portable Computers."

Devising a Home Folder Distribution Strategy

Determine which users need home folders and identify the computers on which you want users' home folders to reside. For performance reasons, avoid using network home folders over network connections slower than 100 Mbit/s.

A user's network home folder doesn't need to be stored on the same server as the directory containing the user's account. In fact, distributing directory domains and home folders among various servers can help you balance your network load. "Distributing Home Folders Across Multiple Servers," on page 103, describes such a scenario.

You may want to store home folders 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 folders on a Mac OS X Server computer but store user and group accounts on an Active Directory or LDAP server.

Pick a distribution strategy before creating users. If your distribution strategy fails while using it, you can move home folders, but doing so may require changing a large number of user records.

When determining the access protocol to use for home folders, you usually use AFP because it offers the greatest level of security. If you are hosting home folders on UNIX servers that do not support AFP, you may want to use NFS. If you are hosting home folders on Windows servers, you may want to use SMB/CIFS. For more information about how to use these protocols for home folders, see "About Home Folders" on page 101.

Identifying Groups

Identify users with similar requirements and consider assigning them to groups. See Chapter 5, "Setting Up Group Accounts."

Determining Administrator Requirements

Decide which users you want to be able to administer accounts, and make sure they have domain administrator privileges.

The domain administrator has the greatest amount of control over other users and their privileges. The domain administrator can create user accounts, group accounts, and computer lists, 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) administrator privileges within certain directory domains.

Give some thought to which users require domain administrator privileges. Managed users can be given various administrator privileges also, allowing them to manage specific groups of users or adjust certain account settings. A well-planned hierarchy of administrators and users with special administrator privileges can help you distribute system administration tasks and make workflow and system management more efficient.

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. Many server administrators don't need to know the root password, but sometimes it's necessary when using command-line tools (such as `CreateGroupFolder`). For administrators who don't need root access, use Workgroup Manager to create an administrator user with a password that is different from the root password.

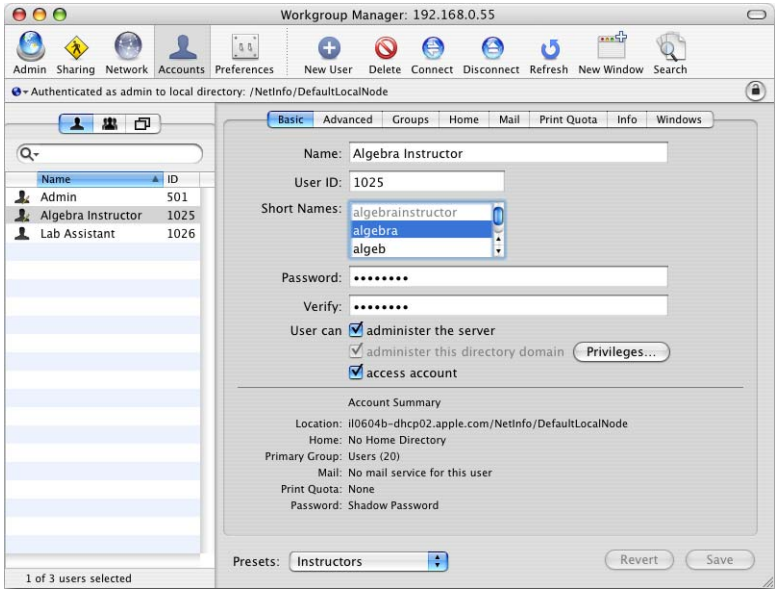
The root password should be used with caution and stored in a secure location. The root user has full access to the system, including system files. If you need to, you can use Workgroup Manager to change the root password.

Getting Started with Workgroup Manager

3

This chapter provides instructions for setting up Workgroup Manager and using some of its core features.

Workgroup Manager is the main application for managing client computers. You can use Workgroup Manager to create accounts, manage preferences, and create and manage share points and network views.



Configuring the Administrator's Computer and Account

In order to use Workgroup Manager, you first need to install the Mac OS X Server administration tools. Before you can manage client computers, you need to configure a computer for use as an administrator computer and create a domain administrator account.

Setting Up an Administrator Computer

By installing Workgroup Manager and other administration tools on a remote administrator computer, you do not need to physically access the server. Instead, you use this administrator computer to connect to the server and perform any administrative tasks you require.

In order to create and modify accounts, you also need to have a domain administrator account.

To set up an administrator computer:

1. Obtain a computer with Mac OS X version 10.4 or later installed.

   Make sure it has at least 256 MB of RAM and 1 GB of unused disk space. For a more detailed description of server and storage requirements, see "Determining Server and Storage Requirements" on page 34.

2. Insert the Mac OS X Server Administration Tools disc, and then start the installer (ServerAdministrationSoftware.mpkg, located in the /Installers folder).

   Make sure you install the same version of the server administration tools as the version of Mac OS X Server installed on your servers. If you use older server administration tools with a newer server version, the tools could cause errors and corrupt data.

3. Follow the onscreen instructions.

4. If you'll be managing preferences that use specific paths to find files (such as Classic and Dock preferences), make sure the administrator computer has the same file system structure as each of the managed client computers. This means that folder names, volumes, the location of applications, and so forth should be the same.

Creating a Domain Administrator Account

Before you can create and edit accounts in a shared directory, you need a domain administrator account in the directory. A domain administrator can use Workgroup Manager to add and change accounts that reside in the LDAP directory of an Open Directory master, a NetInfo domain, or another read/write directory domain.

To create a domain administrator account:

1. On the administrator computer, open Workgroup Manager, authenticating as the administrator user created during initial server setup.

2. Access the shared directory by clicking the globe.

   Choose the directory of interest. If you're not authenticated, click the lock and enter the name and password of a directory domain administrator.

3. Click New User.

4. Click Basic to provide basic information for the administrator.

5. If you want the domain administrator to have other responsibilities, such as setting up file services to support shared folders, select "Administer this directory domain."

After you select the checkbox, a dialog appears in which you can disable specific privileges for the administrator account. For more information, see "Assigning Administrator Privileges for a Directory Domain" on page 62.

6 Click Save.

Using Workgroup Manager

Once you have installed the Mac OS X Server software and set up a domain administrator account, you can access and use Workgroup Manager for user management. This section provides an introduction to the application.

Working with Pre–Version 10.4 Computers from Version 10.4 Servers

Servers running Mac OS X Server version 10.3 can be administered using version 10.4 server administration tools. Workgroup Manager on a computer running Mac OS X Server v10.4 can be used to manage Mac OS X clients running Mac OS X v10.2.4 or later.

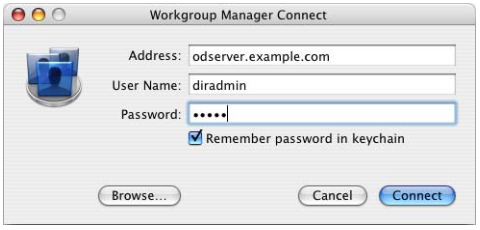
You can only manage preferences for Mac OS 9 clients on Mac OS X Server v10.4 systems by using Macintosh Manager. To install Macintosh Manager, you must perform an upgrade installation from Mac OS X Server version 10.2.8 or 10.3 to Mac OS X Server v10.4.

Once you've edited a user record using Workgroup Manager on Mac OS X Server v10.4, you cannot edit that record using any earlier version of Mac OS X Server.

Connecting and Authenticating to Directory Domains in Workgroup Manager

When you install your server or set up an administrator computer, Workgroup Manager is installed in /Applications/Server/. Use the Finder to open it, or click its icon in the Dock or in the toolbar of the Server Admin application.

- To work with directory domains on a particular server, enter the server's IP address or DNS name in the Workgroup Manager Connect window, or click Browse to choose from a list of available servers. Specify the user name and password for a domain administrator, and then click Connect. Only domain administrators on the directory domain server have directory administrator privileges.



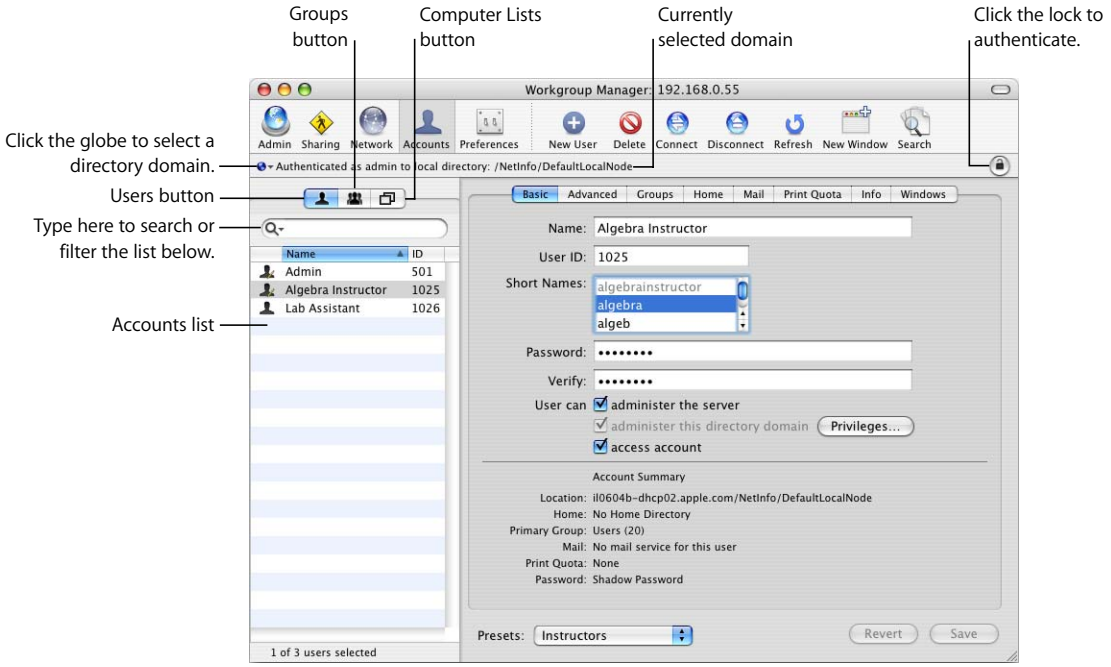
- To change directory domains while connected to a particular server, click the globe to select a domain. You can authenticate as a domain administrator by clicking the lock icon.

- You can view a directory domain without authenticating (by choosing Server > View Directories). You have read-only access to information displayed in Workgroup Manager. To make changes in a directory, you must authenticate using a domain administrator account. This approach is most useful when you're administering different servers and working with different directory domains.

After opening Workgroup Manager, you can open a Workgroup Manager window for a different computer by clicking Connect in the toolbar or choosing Server > Connect.

Major Workgroup Manager Tasks

After login, the accounts pane appears, showing a list of user accounts. Initially, the user accounts listed are those stored in the last directory domain of the server's search policy.



Here is how to get started with the major tasks you perform with Workgroup Manager:

- To specify the directory that stores accounts you want to work with, click the globe icon.
- To work with accounts in different directories at the same time or to work with different views of accounts in a particular directory, open multiple Workgroup Manager windows by clicking the New Window icon in the toolbar.
- To administer accounts in the selected directory, click the Accounts icon in the toolbar. Click the Users, Groups, or Computer Lists button on the left side of the window to list the accounts that currently exist in the directory or directories you are working with. To filter the account list displayed, use the pop-up search menu above the accounts list.
- To work with managed preferences, select the account list of interest and then click the Preferences icon in the toolbar.
- To work with share points, click the Sharing icon in the toolbar.
- To import or export user and group accounts, choose Server > Import, or Server > Export.
- To view onscreen help, use the Help menu. The Help menu gives you access to help for administration tasks you accomplish using Workgroup Manager, as well as other Mac OS X Server topics.
- To open Server Admin so you can monitor and work with services on particular servers, click the Admin icon in the Workgroup Manager toolbar. See the getting started guide for information about Server Admin.

Listing and Finding Accounts

This section describes how you view user accounts, group accounts, and computer lists in Workgroup Manager.

Working with Account Lists in Workgroup Manager

In Workgroup Manager, user accounts, group accounts, and computer lists are listed along the left side of the Workgroup Manager window.

There are several settings that influence the contents and appearance of the list:

- Workgroup Manager preferences control the maximum number of records shown, and whether you want to enable the Inspector, which allows you to view or edit raw directory data. Choose Workgroup Manager > Preferences to set up Workgroup Manager preferences.
- The list reflects the directory you chose from the globe pop-up menu. If you connect to the directory server, the parent directory domain accounts are listed initially. If you do not connect to the directory server, local accounts are listed initially.

The listed domains are the local directory, all directory domains in the server's search policy, and all available directory domains (domains the server is configured to access, even if not in the search policy). See the Open Directory administration guide for instructions on configuring a server to access directory domains.

After you choose directory domains, all the accounts residing in those domains are listed.

- You can list users, groups, or computer lists by clicking the Users, Groups or Computer Lists buttons above the search filter.
- To sort a list, click a column heading. An arrow shows the sort order (ascending or descending), which you can reverse by clicking the column heading again.
- You can search for specific items in the list by typing in the field above the accounts list. Use the pop-up search filter to choose the search criteria.

To work with one or more of the accounts listed, select them. Settings for the selected accounts appear in the pane to the right of the list. Available settings vary, depending on which pane you're currently viewing.

Listing Accounts in the Local Directory Domain

Services and programs running on a server can access the server's local directory. Programs running on a client computer, such as the client computer's login window, can't access the server's local directory. If a server hosts file services, users with accounts from the server's local directory can authenticate with the file services. User accounts from the server's local directory can't be used to authenticate in the login window on client computers, because the login window is a process running on the client computer.

To list accounts in a server's local directory domain:

1. In Workgroup Manager, connect to the server hosting the domain, and then click the globe and choose Local.

   The local domain might also be listed as /NetInfo/root/*host name* or /NetInfo/DefaultLocalNode.

2. To view user accounts, click the Users button. Click the Groups button to view group accounts, or click the Computer Lists button to view computer lists.
3. To work with a particular account, select it. Changing the account requires domain administrator privileges, so you may need to click the lock to authenticate.

Listing Accounts in Search Policy Directory Domains

The search policy directory domains are those in the search policy defined for the Mac OS X Server computer you're connected to. The Open Directory administration guide explains how to set up search policies.

To list accounts in search policy domains of the server you're working with:

1. In Workgroup Manager, connect to a server whose search policy contains the directory domains of interest.
2. Click the globe and choose Search Policy from the globe pop-up menu.
3. To view user accounts, click the Users button. Click the Groups button to view group accounts, or click the Computers button to view computer lists.

Listing Accounts in Available Directory Domains

Using Workgroup Manager, you can list user accounts, group accounts, and computer lists residing in any available directory domain accessible from the server you're connected to. You select the domain from a list of all the directory domains accessible from the server you're using.

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. However, the same server might be configured to access directory domains that haven't been added to its search policy.

See the Open Directory administration guide to learn how to configure access to directory domains.

To list accounts in directory domains accessible from a server:

1. In Workgroup Manager, connect to a server from which you can access the directory domains.
2. Click the globe and choose Other from the globe pop-up menu.
3. In the dialog that appears, select the domains, and then click OK.

   To view user accounts residing in the selected directory domains, click the Users button. Click the Groups button to view group accounts, or click the Computer Lists button to view computer lists.
4. To work with a particular account, select it. To change an account that requires domain administrator privileges, you may need to click the lock to authenticate.

Refreshing Account Lists

If more than one administrator can make changes to directory domains, make sure you're viewing the most current list of user accounts, group accounts, and computer lists by refreshing the lists. To refresh the lists:

- Click Refresh.
- Type search terms in the field above the list to view a new filtered list.
- Delete terms in the field above the list to show the original unfiltered list.
- Click the globe and choose another item in the globe pop-up menu, and then reselect the domains you were working with.

Finding Specific Accounts in a List

After you've displayed a list of accounts 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, click the Users, Groups, or Computer Lists button.
2. In the search pop-up menu, select an option to describe what you want to find, and then type search terms in the search field.

   The original list is replaced by items that satisfy your search criteria. If you type a user name, both full and short names of users are searched. If you type a group name, short names of groups are searched.
3. Choose Workgroup Manager > Preferences to make finding accounts more convenient when the domains you work with contain thousands of accounts.

   To avoid listing any accounts until a filter is specified, select "Limit search results to requested records." When the search field is empty, no accounts are listed. To list all accounts in the selected directory domain, type "*" (without quotes) in the search field.

   To specify the maximum number of accounts to list, select "List a maximum of *n* records," and enter a number no greater than 25,000. Workgroup Manager can display a maximum of 25,000 accounts.

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 sort order.

Using the Search Button in the Toolbar

The Search button can be used in the Accounts or Preferences panes to locate specific users or groups by searching for fields relevant to them.

To locate specific users or groups in the Accounts or Preferences panes:

1. In Workgroup Manager, select the pane you want to work in and click Search in the toolbar.
2. Enter the text you want to search, along with any additional conditions.
3. You can choose to save, rename, or delete a preset by using the Search Presets pop-up menu.

   You can perform a batch edit on the search results. If you select this option, you can choose to "preview and edit search results before applying changes" or "display postview of changes or errors." Previewing the search results creates a list of the accounts that are affected when you save batch edits. Displaying a postview creates a list of the accounts and the changes made to each of those accounts after saving batch edits.

4 Click Search Now after you define your search criteria.

Once you get your search results, you can either clear the search to revert to your default display, or edit the search to refine it further. You can also save a search as a preset for later use.

Shortcuts for Working with Accounts

To manage accounts more efficiently, you can:

- Make changes to multiple accounts at once.
- Use presets, which are like templates for new accounts.
- Import user and group account information from a file.

Editing Multiple Accounts Simultaneously

You can edit settings (if they don't need to be unique) for multiple user accounts, group accounts, or computer lists at the same time. Simultaneously editing multiple accounts is referred to as *batch editing*.

To select multiple accounts, hold down the Shift key while clicking to select a range of accounts. You can also hold down the Command key and then click to select accounts individually. You can also choose Edit > Select All, and then Command-click to deselect particular accounts.

Alternatively, you can use the Search button in the toolbar to find records that match your criteria. You can then select "Perform a batch edit on the search results."

An example of how batch editing can save you time is when you need to change preference settings for a large number of accounts. For more information, see "Editing Preferences for Multiple Records" on page 147.

Using Presets

You can select settings for a user account, group account, or computer list and save them as a preset. Presets work like templates, allowing you to apply predefined settings to a new account. Using presets, you can easily set up multiple accounts with similar settings.

You can use presets only during account creation. You can't use a preset to modify an existing account. You can use presets when creating accounts manually, or when importing them from a file.

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.

For more information about how to create presets, see "Creating a Preset for User Accounts" on page 55.

Importing and Exporting Account Information

You can use XML or character-delimited text files to import and export user and group account information. Importing information can make it easier to set up a large number of accounts quickly. Exporting information to a file is useful for record keeping. To back up account information with passwords intact, archive the directory.

For more information, see Appendix A, "Importing and Exporting Account Information."

Backing Up and Restoring User Management Data

With Workgroup Manager, you can quickly back up and restore directory domains, authentication database files, and user account information.

Backing Up and Restoring Directory Domain and Authentication Files

See the Open Directory administration guide for information about backing up directory domains and authentication database files. See onscreen help for information about restoring directory domains and authentication database files.

Backing Up Root and Administrator User Accounts

System files are owned by root or local administrator user IDs that exist at the time they're created. Should you need to restore system files, the same IDs should exist on the server so that the original permissions are preserved.

To ensure that you can re-create these user IDs, periodically export the server's user and group information to a file. Exporting account information is described in Appendix A, "Importing and Exporting Account Information."

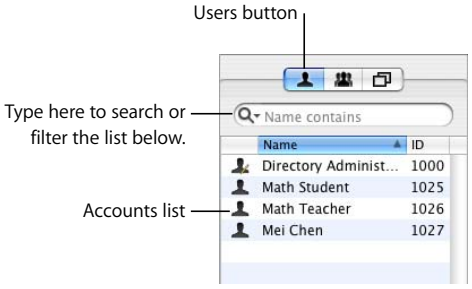
Setting Up User Accounts

4

This chapter tells you how to set up, edit, and manage user accounts.

If you want to manage individual users or if you want those users to have unique identities on your network, create user accounts.

You can use Workgroup Manager to view, create, edit, and delete user accounts. You can view user accounts in Workgroup Manager by clicking the Users button above the accounts list.



About User Accounts

A user account stores data that Mac OS X Server needs to validate the user's identity and provide services to the user. This section provides an overview of user accounts.

Where User Accounts Are Stored

User accounts, as well as group accounts and computer lists, can be stored in any Open Directory domain accessible from any Mac OS X computer. A directory domain can reside on a Mac OS X computer (for example, the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain) or it can reside on a non-Apple server (for example, a non-Apple 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 the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain using Workgroup Manager.

For complete information about the different kinds of directory domains, see the Open Directory administration guide.

Predefined User Accounts

The following table describes some of the user accounts that are created automatically when you install Mac OS X Server (unless otherwise indicated). For a complete list, open Workgroup Manager and choose View > Show System Users and Groups.

Predefined user name	Short name	User ID	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 doesn't already exist.
My SQL Server	mysql	74	The user that the MySQL database server uses for its processes that handle requests.
Sendmail User	smmsp	25	The user that sendmail runs as.
sshd Privilege separation	sshd	75	The user for the sshd child processes that process network data.
System Administrator	root	0	The most powerful user.
System Services	daemon	1	A legacy UNIX user.
Unknown User	unknown	99	A user with no login or password. When files or volumes have no real owner, they are assigned unknown as their owner.
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.

Administering User Accounts

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

Creating Mac OS X Server User Accounts

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

To create user accounts in an LDAPv3 directory on a non-Apple server, first use Directory Access to map the LDAPv3 directory's attributes to Open Directory user and group attributes. For more information about user account elements that may need to be mapped, see "Understanding What You Can Import and Export" on page 231.

To create users in an Active Directory domain, use Active Directory administration tools on a Windows computer. Workgroup Manager can't be used to create user accounts, group accounts, or computer lists in a standard Active Directory domain. If you extend the schema of the Active Directory domain, you can create computer lists in Active Directory.

For detailed instructions on mapping LDAPv3 attributes or connecting to Active Directory, see the Open Directory administration guide.

To create a user account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   See the Open Directory administration guide for instructions.
3. Click the globe, and then choose the domain in which you want the user's account to reside.

   Local, /NetInfo/root/*host name*, and /NetInfo/DefaultLocalNode all refer to the local directory domain. /NetInfo/root refers to a shared NetInfo domain if the server is set up to access one; otherwise, /NetInfo/root is the local domain.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Choose Server > New User, or click New User in the toolbar.
6. Specify settings for the user in the panes provided.

   For details, see "Working with Basic Settings" on page 57 through "Working with Print Settings" on page 72.

   You can also use a preset or an import file to create a new user. For details, see "Using Presets to Create New Accounts" on page 55 and "Using Workgroup Manager to Import Users and Groups" on page 232.

Editing User Account Information

You can use Workgroup Manager to change a user account that resides in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain.

To make changes to a user account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server you're using have been configured to access the desired directory domain.

   See the Open Directory administration guide for instructions.
3. Click the globe, and then choose the domain where the user's account resides.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Users button and select the user account.
6. Edit settings for the user account in the panes provided.

   For details, see "Working with Basic Settings" on page 57 through "Working with Print Settings" on page 72.

Editing Multiple User Accounts Simultaneously

You can use Workgroup Manager to simultaneously apply the same settings to multiple user accounts in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain.

Although you can simultaneously edit most account settings for multiple users, there are several account settings that you can only change per user. For example, you cannot assign the same name, short name, or user ID to multiple users. Workgroup Manager disables fields where you are expected to provide unique values.

To edit multiple user accounts:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon below the toolbar and choose the directory domain where the user accounts that you want to edit reside.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Select the user accounts you want to edit.

   Hold down the Command key while clicking to select multiple user accounts, or hold down the Shift key while clicking to select a range of accounts.
5. Edit fields in the panes within Accounts.

   If a field is disabled, you cannot edit this field while multiple user accounts are selected.

Modifying Accounts in an Open Directory Master

You can modify accounts in the LDAP directory of an Open Directory master if you're authorized to administer the directory domain but not the server itself. Your user ID must have "User can Administer this directory domain" selected in the Basic pane of Accounts in Workgroup Manager.

If you do not have this privilege, you have to authenticate to the directory domain with the Directory Administrator account that gets created in Mac OS X Server when you specify your server to be a directory master in the Server Admin utility. The UID, user name, and password of the Directory Administrator account (which defaults to the modifiable UID of 1000 and user name "diradmin") is set by the server administrator at the time of directory creation.

To modify accounts:

1. Use an administrator computer that has been set up (using the Services pane of Directory Access) to access the server hosting the Open Directory master.
2. Open Workgroup Manager on the administrator computer.
3. When the login window appears, choose Server > View Directories.
4. Click the globe and choose Other from the pop-up menu.
5. Open the directory domain you want to administer, and then click the lock and enter the name and password of a directory domain administrator.

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. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the directory domain where the account resides.

   For information about using Directory Access to configure server connections, see the Open Directory administration guide. For information about the user account elements that need to be mapped, see Appendix A, "Importing and Exporting Account Information."
3. Click the globe and choose the directory domain in which the user's account resides.
4. Use the panes provided to review the user's account settings.

   For details, see "Working with Basic Settings" on page 57 through "Working with Print Settings" on page 72.

Working with Guest Users

You can set up some services to support "anonymous" users, who can't be authenticated because they don't have a valid user name or password. The following services can be set up to support guest access by anonymous users:

- **Windows services.** See the Windows services administration guide.
- **Apple file service.** See the file services administration guide.
- **FTP service.** See the file services administration guide.
- **Web service.** See the web technologies administration guide.

Users who connect to a server anonymously are restricted to files, folders, and websites with permissions set to Everyone.

Another kind of guest user account is a managed user account that you can define to allow easy setup of public computers or kiosk computers. For more about these kinds of user accounts, see Chapter 10, "Managing Preferences," on page 137.

Deleting a User Account

You can use Workgroup Manager to delete a user account stored in the LDAP directory of an Open Directory master or a NetInfo domain, or from any other read/write directory domain.

> *Warning:* You cannot undo this action.

To delete a user account using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to delete.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Choose Server > Delete Selected User, or click the Delete icon in the toolbar.

Disabling a User Account

To disable a user account, you can:

- Deselect the "User can log in" option in the Basic pane in Workgroup Manager.
- Delete the account.
- Change the user's password to an unknown value.
- Set a password policy that disables login. This applies only to user accounts whose password type is Open Directory.

Working with Presets

Presets are templates you use to define attributes that automatically apply to new user or group accounts.

Creating a Preset for User Accounts

You can create one or more presets to choose from when creating new user accounts in a particular directory domain.

To create a preset for user accounts:

1. Open Workgroup Manager on the server from which you are going to create user accounts.

   Ensure that the server has been configured to access the Mac OS X directory domain or non-Apple LDAPv3 domain in which you are going to use the preset to create new accounts. To access a different domain, click the globe.

2. Click Accounts.

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 don't want to prespecify if you're basing the preset on an existing account.

   The following attributes can be defined in a user account preset: password settings, administrator privileges, home folder settings, quotas, default shell, primary group ID, group membership list, comment, login settings, print settings, and mail settings.

   You might want to set up password options so that users are forced to change their password the next time they log in. This is especially useful when you import user accounts. For instructions on how to require a password change at next login, see "Choosing a Password Type and Setting Password Options" on page 64.

5. Click Preferences, configure settings that you want the preset to define, and then click Accounts.

   After configuring preference settings for a preset, you must return to the Accounts settings to save the preset.

6. Choose Save Preset from the Presets pop-up menu, enter a name for the preset, and then click OK.

   The preset is saved to the current directory domain.

Using Presets to Create New Accounts

Presets provide a quick way to apply settings to a new account. After you apply the preset, you can continue to modify settings for the new account, if necessary.

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 domain in which you are going to use the preset to create the new account.

2. Click Accounts.

3 Click the globe above the accounts list, and then choose the directory domain in which you want the new account to reside.

4 To authenticate, click the lock and enter the name and password of a directory domain administrator.

5 Choose an item from the Presets pop-up menu. If you plan to import a file, choose a preset in the import options dialog.

6 Create a new account, either interactively or using an import file.

If a setting is specified in both the preset and an import file, the value in the file is used. If a setting is specified in the preset but not in the import file, the value in the preset is used.

7 Add or update attribute values if required, either interactively or using an import file.

Renaming Presets

Name your presets to help remind you of the template settings or identify the type of user account, group account, or computer list for which that preset is best suited. You can rename your presets.

To rename a preset:

1 Open Workgroup Manager on the server where the preset has been defined.

2 Click Accounts.

3 Choose Rename Preset from the Presets pop-up menu.

4 Enter the new name and click OK.

Editing 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 Accounts.

3 Choose an item from the Presets pop-up menu.

4 After completing your changes, choose Save Preset from 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, and then saving the preset.

Deleting a Preset

If you no longer need a particular preset, you can delete it.

To delete a preset:

1 Open Workgroup Manager on the server where the preset has been defined.

2 Click Accounts.

3 Choose Delete Preset from the Presets pop-up menu.

4 Select the preset you want to delete and click Delete.

Working with Basic Settings

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

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

Defining User Names

The user name is the long name for a user, such as Mei Chen or Dr. Anne Johnson. (Sometimes the user name is referred to as the "full name" or the "real" name.) Users can log in using the user name, or a short name associated with their accounts.

A user name can contain no more than 255 bytes. Since long user names support various character sets, the maximum number of characters for long user names can range from 255 Roman characters to as few as 85 characters (for character sets in which characters occupy up to 3 bytes).

You can use Workgroup Manager to edit the user name of an account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the user name in any directory domain accessible from the server you're using.

To work with the user name using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 In the Name field (in the Basic pane), review or edit the user name.

Initially, the value of the user name is "Untitled #," where # is the number sequentially generated after the last generated number for a saved untitled user. After changing the name, Workgroup Manager doesn't check to verify that the user name is unique.

Avoid assigning the same name to more than one user. Workgroup Manager doesn't let you assign the same name to different users in any particular domain or in any domain in the search policy (search policy) of the server you're using, but has no way of detecting whether duplicates might exist in other domains.

Defining Short Names

A *short name* is an abbreviated name for a user, such as mchen or annejohnson. 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 folders.

When Mac OS X creates a user's local or network AFP home folder, it names the directory after the user's short name. For more information about home folders, see Chapter 7, "Setting Up Home Folders."

You can have as many as 16 short names associated with a user account. You might want to use multiple short names as aliases for email accounts, for example. The first short name is the name used for home folders and legacy group membership lists; don't reassign that name after you save the user account.

A short user name can contain as many as 255 Roman characters. However, for clients using Mac OS X version 10.1.5 and earlier, the first short user name must be 8 characters or fewer.

Use only these characters for the first short user name (subsequent short names can contain any Roman character):

- a through z
- A through Z
- 0 through 9
- _ (underscore)

Typically, short names contain eight or fewer characters.

You can use Workgroup Manager to edit the short name of an account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the short name in any directory domain accessible from the server you're using.

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

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the Short Names field (in the Basic pane), review or edit the short names.

   Initially, the value of the short name is "untitled_#," where # is the number sequentially generated after the last generated number for a saved untitled user. If you specify multiple short names, each should be on its own line.

Avoid assigning the same short name to more than one user. Workgroup Manager doesn't let you assign the same short name to different users in any particular domain or in any domain in the search policy of the server you're using, but has no way of detecting whether duplicates might exist in other domains.

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

Choosing Stable Short Names

You cannot use the Basic pane of Workgroup Manager to change the first short name for a user.

If you need to change the first short name, 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 (user ID, primary group, home folder, and so forth). You can 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 54 for information about how to disable use of an account for login.

Mac OS X version 10.4 introduces globally unique identifiers (GUIDs) for determining group membership. In previous versions of Mac OS X, group membership was determined by the user's first short name. If you delete a user and re-create the user with the same short name, group memberships are not retained.

For more information about GUIDs, see Appendix B, "ACL Permissions and Group Memberships Using GUIDs."

Avoiding Duplicate Names

A user account's short name is used by the login window, so multiple users with the same short name will cause a conflict. Although you cannot create multiple users with the same short name in the Basic pane of Workgroup Manager, it is still possible to create multiple users with the same short name when you use command-line tools or Workgroup Manager's Inspector interface.

If multiple user accounts have the same long user name on a Mac OS X computer, login window displays the list of users for you to choose from. This functionality is new to Mac OS X version 10.4. Previous versions of Mac OS X do not display this list.

If two users have the same first short user name, the login window only recognizes, and authenticates the first matching user account it finds in the sequence of directory domains specified by the computer's search policy, as set in Directory Access. If a local user and a network user have the same first short user name, the local user always take precedence. This prevents the network user from logging in to the computer.

In groups created in Mac OS X versions earlier than 10.4, group membership is determined by the user's first short name and group ID (GID). If multiple users have the same first short name, they have the same group memberships. Groups created in Mac OS X Server version 10.4 determine group membership using both a globally unique identifier (GUID) and a combination of the user's short name and GID. For detailed information about GUIDs, see "Understanding GUIDs" on page 239.

If you do not upgrade legacy groups, the groups still determine membership by only the user's first short name and GID. For instructions on upgrading legacy groups, see "Upgrading Legacy Groups" on page 81. It is highly recommended that you avoid using duplicate user short names, in order to allow users to log in to computers and to ensure correct legacy group membership.

Defining User IDs

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

The user ID should be a unique string of digits from 500 through 2,147,483,648. It is risky to assign the same user ID to different users, because two users with the same user ID have identical directory and file permissions.

The user ID 0 is reserved for the root user. User IDs below 100 are reserved for system use; users with these user IDs should not be deleted and should not be modified except to change the password of the root user. If you do not want the user to appear in the login window of computers with Mac OS X version 10.4 or later installed, assign a user ID of less than 500.

In general, once user IDs have been assigned and users start creating files and folders, you shouldn't change user IDs. One possible scenario in which you may need to change a user ID is when merging users created on different servers onto one new server or cluster of servers. The same user ID may have been associated with a different user on the previous server.

When you create a new user account in any shared directory domain, Workgroup Manager automatically assigns a user ID; the value assigned is an unused user ID (1025 or greater) in the server's search policy. (New users created using the Accounts pane of System Preferences are assigned user IDs starting at 501.)

You can use Workgroup Manager to edit the user ID of an account stored in the LDAP directory of an Open Directory master or a NetInfo domain. You can also use Workgroup Manager to review the user ID in any directory domain accessible from the server you're using.

To change a user ID in Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select an account, click the globe above the accounts list and choose the directory domain where the user's account resides, and select the user.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the Basic pane, specify a value in the User ID field.

   Make sure the value is unique for all the directory domains set in the search policy of computers the user logs in to. Workgroup Manager warns you if you change it to a number already assigned to another user in the same directory domain.

Defining Passwords

For information about defining passwords, see the Open Directory administration guide.

Setting Password Options for Imported User Accounts

When you export user accounts using Workgroup Manager, password information isn't exported. If you want to set passwords, you can modify the export file before you import it or you can set passwords after importing. You can also create a text-delimited import file manually and include passwords in it. Appendix A describes how to work with import files.

To set password options after importing:

1. Import the user accounts by using Workgroup Manager or the `dsimport` command-line tool.
2. In Workgroup Manager, click Accounts.
3. Open the directory into which the user accounts were imported.
4. Select the user accounts whose password options you want to set.
5. Click Advanced.
6. Make sure the User Password Type is set to Open Directory. Then click Options, set password options, and click OK.
7. Click Save.

For more information about importing user accounts, see "Understanding What You Can Import and Export" on page 231. For additional information about Open Directory passwords, see the Open Directory administration guide.

Assigning Administrator Privileges 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 Admin, 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 the LDAP directory of an Open Directory master or a NetInfo domain. You can also use Workgroup Manager to review the server administrator privileges in any directory domain accessible from the server you're using.

To set server administrator privileges in Workgroup Manager:

1. 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 Accounts.
3. Click the globe and choose Local.
4. Click the lock and enter the name and password of a local administrator.
5. Click the globe and choose the directory domain in which the user's account resides.
6. Click the lock and enter the name and password of a directory domain administrator.
7. In the Basic pane, select "User can administer the server" to grant server administrator privileges.

Assigning Administrator Privileges for a Directory Domain

A user who has administrator privileges for an Apple directory domain can make changes to user accounts, group accounts, and computer lists 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 to an account stored in the LDAP directory of an Open Directory master or a NetInfo domain. You can also use Workgroup Manager to review these privileges in any directory domain accessible from the server you're using.

To set directory domain administrator privileges in Workgroup Manager:

1. Make sure the user has an account in the directory domain.
2. In Workgroup Manager, click Accounts.
3. Select the user account.

   To select the account, click the globe and choose the directory domain in which the user's account resides, and select the account.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. In the Basic pane, select "User can administer this directory domain."

6 To specify what the user can administer in the domain, click Privileges.

By default, the user has no directory domain privileges.

7 Click the Users, Groups, or Computer Lists button and make the desired settings.

If you don't select a checkbox (such as "The administrator can edit user preferences"), the user can view the account or preference information in Workgroup Manager, but cannot change it.

To add an item to the "listed below" area on the right, drag it from the Available list on the left. To remove an item, select it and press the Delete key.

Working with Advanced Settings

Advanced settings include login settings, keywords, password validation policy, and a comment field. In Workgroup Manager, use the Advanced pane 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.
- Identify the default shell the user uses for command-line interactions with Mac OS X, such as /bin/csh or /bin/bash (the default). 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 for an account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review login settings for any directory domain accessible from the server you're using.

To work with login settings using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and then select the user account.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click Advanced.

5 Select "Allow simultaneous login on managed computers" to let a user use the login window to log in to more than one managed computer at a time.

Note: Simultaneous login is not recommended for most users. You may want to reserve simultaneous login privileges for technical staff, teachers, or other users with administrator privileges. (If a user has a network home folder, that's where the user's application preferences and documents are stored. Simultaneous login may modify these items; many applications don't support such modification while they are open.)

You can only disable simultaneous login for users with AFP home folders.

6 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.

Note: Terminal has a preference that lets the user override the default shell.

To enter a shell that doesn't appear in the list, click Custom. To make sure a user can't access the server remotely using the command line, choose None.

Choosing a Password Type and Setting Password Options

For user accounts in the LDAP directory of an Open Directory server, you can set the password type to Open Directory or Crypt Password. User accounts in the local directory domain of Mac OS X Server v10.4 have a password type of Shadow Password.

When you set the password type to Shadow Password or Open Directory, you can set several password policy options, including disabling login after a period of inactivity or failed authentication attempts, or setting password restrictions such as requiring that passwords be of a certain length or that they be changed at next login. If you set the password type to Shadow Password, you can also set security options to control which authentication methods are used when validating the user's password.

For a detailed explanation of password types, password policy options, and security options, see the Open Directory administration guide.

To choose a user password type and set available options:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click Advanced.

5 Choose Shadow Password, Open Directory, or Crypt Password from the User Password Type pop-up menu.

When you choose a password type, a prompt requiring you to enter a password might appear, depending on whether you entered a password in the Basic pane. If you chose Open Directory, an Options button appears. You can change this password in the Basic pane.

6 If you choose Open Directory or Shadow Password, you can set a password policy for the selected user or users by clicking Options. Select any of the options to enable them. Click OK.

7 If you choose Shadow Password, you can also select authentication methods by clicking Security.

8 Click Save.

Creating a Master List of Keywords

You can define keywords that enable quick searching and sorting of user accounts. Using keywords can simplify tasks such as creating groups or editing multiple user accounts.

Before you begin adding keywords to user records, you must create a master keyword list. The list of keywords shown in the Advanced pane for a selected user applies only to that user.

To edit the master keyword list:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click Advanced.

5 Click the Edit (pencil) button to view the master keyword list.

The master list shows all terms available for use as keywords. You can access and edit the master keyword list from any selected user account.

6 To add a keyword to the master list, click Add (+) and type the keyword in the text field.

7 To remove a keyword from the master list and from all user records where it appears, select the keyword, select "Remove deleted keywords from users and computers," and click Remove (–).

If you only want to remove a keyword from the master list, make sure "Remove deleted keywords from users and computers" is not selected, and then select the keyword you want to remove and click Remove (–).

8 When you've finished editing the master list, click OK.

Applying Keywords to User Accounts

You can't add keywords to more than one user account at a time; however, you can remove a keyword from all user accounts that are tagged with that keyword if necessary.

To work with keywords for an individual user account:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Advanced.
5. To add a keyword to the selected account, click Add (+) to view the list of available keywords. Select one or more keywords in the list, and then click OK.
6. To remove a keyword from a specific user account, select the keyword you want to remove and click Remove (–).
7. When you've finished adding or removing keywords for the selected user account, click Save.

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 the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the comment in any directory domain accessible from the server you're using.

To work with a comment using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Advanced.
5. Edit or review the contents of the Comment field.

Working with Group Settings

Group settings identify the groups a user is a member of. In Workgroup Manager, use the Groups pane in the user account window to work with group settings.

For information about how to administer group accounts, see Chapter 5, "Setting Up Group Accounts."

Defining a User's Primary Group

A *primary group* is the group to which a user belongs to if the user does not belong to any other groups. If a user selects a different workgroup at login, the user still retains access permissions from the primary group.

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

> ***Warning:*** Although you can make a primary group a nested group, or a parent of nested groups, the file permissions for the primary group do not propagate. If a user's primary group is a nested group or the parent of a nested group, the user is granted file permissions only for the primary group. You should not rely on using primary group membership when assigning file permissions.

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 2,147,483,648.

You can use Workgroup Manager to define the primary group ID of an account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the primary group information for any directory domain accessible from the server you're using.

To work with a primary group ID using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Groups button.

5 Edit or review the contents of the Primary Group ID field. Workgroup Manager displays the full and short names of the group after you enter a primary group ID if the group exists and is accessible in the search policy of the server you're logged into.

Adding a User to Groups

Add a user to a group when you want multiple users to have the same file permissions or when you want to manage their Mac OS X preferences using workgroups or computer lists. An example might be students in a classroom who are disallowed from using the printer, or the quality control team in a factory where the team requires access to the internal reports of different groups.

You can use Workgroup Manager to add a user to a group, if the user and group accounts are in the LDAP directory of an Open Directory master or a NetInfo domain. In case the directory is implemented through NFS, a 16-group limitation is imposed by the NFS architecture.

Note: There is no limit to the number of groups a user may belong to.

To add a user to a group using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click the Groups button.

5 Click the Add (+) button to open a drawer listing the groups defined in the directory domain you're working with.

6 Select the group, and then drag it into the Other Groups list in the Groups pane.

You can also add users to a group by using the Members pane of the group accounts window.

Note: If a user is a direct member of multiple groups, the only way to acquire the managed preferences of a group different from its primary group is at login time.

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 the LDAP directory of an Open Directory master or a NetInfo domain.

To remove a user from a group using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click the Groups button.

5 Select the group or groups from which you want to remove the user, and then click the Remove (–) button.

You can also add users to a group by using the Members pane of group accounts.

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're using.

To review group memberships using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the account you want to work with.

To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click the Groups button.

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

Home settings describe a user's home folder attributes. For information about using and setting up home folders, see Chapter 7, "Setting Up Home Folders."

Working with Mail Settings

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 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 pane in the user accounts window to work with a user's mail service settings.

See the mail service administration guide for information about how to set up and manage Mac OS X Server mail service.

Enabling Mail Service Account Options

You can use Workgroup Manager to enable mail service and set mail options for a user account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the mail settings of accounts stored in any directory domain accessible from the server you're using.

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

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Mail.
5. To allow the user to use mail service, select Enabled.
6. Enter a valid mail server name or address in the Mail Server fields for the DNS name or IP address of the server to which the user's mail should be routed. Workgroup Manager doesn't verify this information.
7. Enter a value in the Mail Quota field to specify the maximum number of megabytes for the user's mailbox. A 0 (zero) or empty 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. The message shows quota information in kilobytes (KB) or megabytes (MB).
8. Select a Mail Access setting, to identify the protocol used for the user's mail account: Post Office Protocol (POP) and/or Internet Message Access Protocol (IMAP).
9. The following features are supported only for mail accounts that reside on a server using Mac OS X Server software earlier than version 10.3.

   Select an Options setting to determine 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.

Select "Enable NotifyMail" to 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.

Disabling a User's Mail Service

You can use Workgroup Manager to disable mail service for users whose accounts are stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain.

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

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Mail.
5. Select None.

Forwarding a User's Mail

You can use Workgroup Manager to set up email forwarding for users whose accounts are stored in the LDAP directory of an Open Directory master or a NetInfo domain.

To forward a user's mail using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Mail.
5. Select Forward and enter the forwarding email address in the Forward To field.

   Make sure you enter the correct address. Workgroup Manager doesn't verify that the address exists.

Working with Print Settings

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. The print service administration guide tells you how to set up quota-enforcing print queues.

In Workgroup Manager, use the Print Quota pane in the user accounts window to set a user's print quotas. Select:

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

Enabling a User's Access to Print Queues that Enforce 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 the LDAP directory of an Open Directory master or a NetInfo domain.

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

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Print Quota button.

   To set up a quota that applies to all queues, go to step 5. Alternatively, to set up quotas for specific print queues, go to step 6.
5. Click "All Queues," then specify the maximum number of pages the user can print in a certain number of days for any print queue enforcing quotas.
6. Click "Per Queue," then use the Queue Name pop-up menu to select the print queue you want to define a user quota for. 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 can print in a certain number of days. Then click Save.

Disabling a User's Access to Print Queues that Enforce 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 the LDAP directory of an Open Directory master or a NetInfo domain.

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

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Print Quota button.
5. Select None.

Deleting a User's Print Quota for a Specific Queue

If you no longer require a print quota for a particular queue and you've set print queue quotas, you can delete that quota for specific users.

To delete a user's print quota using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user in the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Print Quota button.
5. Use the Queue Name pop-up menu and the Print Server field to identify the print queue you want to disable the user's access to.
6. Click Delete.

Resetting a User's Print Quota

Occasionally, a user may exceed his or her print quota but needs to print additional pages. For example, an administrator may want to print a 200-page manual, but the print quota is only 150 pages. Or, a student may exceed the quota by printing an essay but needs to print a new revised copy. You can use Workgroup Manager to reset a user's print quota and allow the user to continue printing.

To restart a user's print quota using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the account you want to work with.

   To select the account, click the globe and choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Print Quota button.
5. 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 the print queue, and then click Restart Print Quota.

   You can also extend a user's page limit without resetting the quota time period by changing the number of pages allowed for the user. In this way, the time period for the quota remains the same and is not reset, but the number of pages the user can print during that period is adjusted for both the current and future print quota periods. To extend or decrease a selected user's page limit, type a new number in the "Limit to ___ pages" field and click Save.

Working with Info Settings

If a user's account resides in an LDAPv3 directory domain, it can contain information imported from Address Book. Attributes that are currently tracked in the Info pane include phone number, email address, weblog URL, and homepage URL.

Note: There is only one phone attribute, and that defaults to the work number in Address Book.

To work with Info Settings:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   See the Open Directory administration guide for instructions.
3. Click the globe, and then choose the domain in which the user's account resides.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Users button and select the user.
6. Click Info, enter or change values as required, and click Save when you are finished.

Choosing Settings for Windows Users

Computers that use the Windows operating system can be integrated into your Mac OS X Server network. You can set up user accounts and select settings in the Windows pane of Workgroup Manager for individuals who need access to the Windows computers.

For detailed instructions about how to use settings for users accessing Windows computers, see the Windows services administration guide.

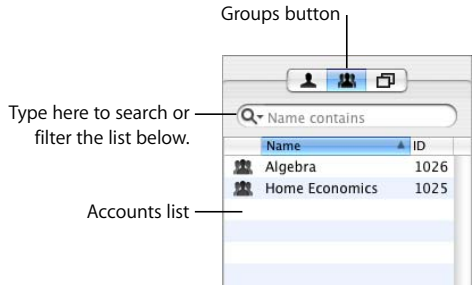
Setting Up Group Accounts

5

This chapter tells you how to set up, edit, and manage group accounts.

A group account offers a simple way to manage a collection of users with similar needs. You can also create group folders, which provide an easy way for group members to share files with each other.

You can use Workgroup Manager to view, create, edit, and delete group accounts. You can view group accounts in Workgroup Manager by clicking the Groups button above the accounts list.



About Group Accounts

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 the group. When you define preferences for a group, the group is known as a *workgroup*.

A *primary group* is the user's default group. Primary groups can expedite the checking done by the Mac OS X file system when a user accesses a file.

Where Group Accounts Are Stored

Group accounts, as well as user accounts and computer lists, can be stored in any Open Directory domain. A directory domain can reside on a Mac OS X computer (for example, the LDAP directory of an Open Directory master or a NetInfo 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. For complete information about the different kinds of Open Directory domains, see the Open Directory administration guide.

Predefined Group Accounts

The following table describes most of the group accounts that are created automatically when you install Mac OS X Server. For a complete list, open Workgroup Manager and choose View > Show System Users and Groups.

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.
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.
sshd	75	The group for the sshd child processes that process network data.
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 disk.
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. Membership is required for using the `su` command.
www	70	The nonprivileged group that Apache uses for its processes that handle requests.

Administering Group Accounts

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

Creating Mac OS X Server Group Accounts

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

You can also create group accounts on a non-Apple LDAPv3 server if has been configured for write access.

To create a group account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   For information about using Directory Access to configure an LDAP connection, see the Open Directory administration guide. For information about the group account elements that may need to be mapped, see Appendix A, "Importing and Exporting Account Information."
3. Click the globe and choose the domain in which you want the group account to reside.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Groups button.
6. Click New Group, and then specify settings for the group in the panes provided.

   You can also use a preset or an import file to create a new group. For details, see "Creating a Preset for Group Accounts" and Appendix A, "Importing and Exporting Account Information."

Creating a Preset for Group Accounts

You can use presets to apply predetermined settings to a new group account.

For instructions on renaming, editing, or deleting group presets, see "Renaming Presets" on page 56, "Editing Presets" on page 56, and "Deleting a Preset" on page 56.

To create a preset for group accounts:

1. Open Workgroup Manager on the server from which you are going to create group accounts.
2. Click Accounts.
3. Ensure that the server has been configured to access the Mac OS X directory domain or non-Apple LDAPv3 domain in which the preset is used to create new accounts.
4. 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.
5. Fill in the fields with values you want new user groups to inherit. Delete any values you don't want to prespecify if you're basing the preset on an existing account.
6. Click Preferences, configure settings that you want the preset to define, and then click Accounts.

   After configuring preference settings for a preset, you must return to the Accounts settings to save the preset.
7. Choose Save Preset from the Presets pop-up menu, enter a name for the preset, and click OK.

Editing Group Account Information

You can use Workgroup Manager to change a group account that resides in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain.

To make changes to a group account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   For instructions, see the Open Directory administration guide.
3. Click the globe and choose the domain in which the group account resides.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Groups button and select the group you want to work with.
6. Edit settings for the group in the panes provided.

   See "Working with Member Settings for Groups" on page 83 and "Working with Group Folder Settings" on page 86 for details.

Creating Nested Groups

A nested group is a group that is a member of another group, known as a parent group.

Nested groups do not inherit managed preferences. Members of a nested group have their preferences managed only by their chosen workgroup, and not by a parent group. The access permissions of a parent group can be inherited. For example, if you set a parent group's ACL permissions so that the parent group cannot write to the folder, you can propagate the ACL permissions so that nested groups also cannot write to the folder.

To create a nested group account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   For instructions, see the Open Directory administration guide.
3. Click the globe and choose the domain in which you want the nested group to reside.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Groups button and create a new group.
6. Click the Add (+) button to nest a group within the selected group. Drag the group from the drawer to the Members list.

   All members of the nested group become members of the parent group as well.
7. Click Save.

   Groups created using server versions prior to Mac OS X Server version 10.4 can't have nested groups unless you convert them as "Upgrading Legacy Groups" describes. If you upgrade from version 10.3 or earlier to version 10.4, groups remain legacy groups and continue to function as they always have. Groups created in Mac OS X v10.4 are considered upgraded groups and can have nested groups and other objects as members, along with user records.

Upgrading Legacy Groups

When you upgrade to Mac OS X Server version 10.4 or import groups created before version 10.4, existing groups can't have nested groups unless you convert them first.

To convert a legacy group account to an upgraded group account:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   For instructions, see the Open Directory administration guide.

3 Click the globe and choose the domain in which the group account resides.

4 To authenticate, click the lock and enter the name and password of a directory domain administrator.

5 Click the Groups button and select the individual legacy group you want to upgrade.

6 Click the Upgrade Legacy Group button.

7 Click Save.

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 In Workgroup Manager, click Accounts.

2 Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the directory domain in which the account resides.

For information about using Directory Access to configure server connections, see the Open Directory administration guide. For information about the group account elements that need to be mapped, see Appendix A, "Importing and Exporting Account Information."

3 Click the globe and choose the directory domain in which the group account resides.

4 Use the panes provided to review the group account settings.

Deleting a Group Account

You can use Workgroup Manager to delete a group account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain.

> *Warning:* You cannot undo this action.

To delete a group account using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to delete.

To select the account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Choose Server > Delete Selected Group or click the Delete icon in the toolbar.

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, you use the Members pane 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 permissions 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 don't need to explicitly do so. Otherwise, you explicitly add users to a group.

You can use Workgroup Manager to add a user to a group if the user and group accounts are in the LDAP directory of an Open Directory master or a NetInfo domain.

To add a user to a group using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select an account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the Members pane, click the Add (+) button to open a drawer listing the users defined in the directory domain you're working with.

   Make sure that the group account resides in a directory domain specified in the search policy of computers the user logs in to.
5. Select the user, and then drag it into the Members list in the Members pane.

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 the LDAP directory of an Open Directory master or a NetInfo domain.

To remove a user from a group using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select an account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Members.
5. Select the user or users you want to remove from the group, and then click the Remove (–) button.

Naming a Group

A group has two names: a long name and a short name.

- The long group name (for example, English Department Students) is used for display purposes only and can contain no more than 255 bytes. Since long group names support various character sets, the maximum number of characters for long group names can range from 255 Roman characters to as few as 85 characters (for character sets in which characters occupy up to 3 bytes).
- A short group name can contain as many as 255 Roman characters. However, for clients using Mac OS X version 10.1.5 or earlier, the short group name must be eight characters or fewer. Use only these characters in a short group name:
  - a through z
  - A through Z
  - 0 through 9
  - _ (underscore)

  The short name, typically eight or fewer characters, may be used by Mac OS X to find user IDs of group members when determining whether a user can access a file as a result of his or her group membership. See Appendix B, "ACL Permissions and Group Memberships Using GUIDs," on page 239 for more information about group membership.

You can use Workgroup Manager to edit the long or short names of a group account stored in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. You can also use Workgroup Manager to review the names in any directory domain accessible from the server you're using.

To work with group names using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select an account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the Name field or the "Short name" field (in the Members pane), review or edit the names.

   Before saving a new name, Workgroup Manager checks to ensure that the name is unique.

Defining a Group ID

A group ID is a string of ASCII digits that uniquely identifies a group. The maximum value is 2,147,483,648.

You can use Workgroup Manager to edit the ID for a group account stored in the LDAP directory of an Open Directory master or a NetInfo domain, or to review the group ID in any directory domain accessible from the server you're using. The group ID is associated with group privileges and permissions.

To work with a group ID using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select an account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the Group ID field (in the Members pane), 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're using.

Working with Group Folder Settings

A group folder offers a way to organize and distribute documents and applications of interest to group members and gives group members a way to share files among themselves.

Group folders are not directly linked to workgroup management, but access and workflow management can be improved by combining the use of group folders with managed preferences for workgroups. For example, to set an multimedia lab computer specifically for a movie-editing class, you could set Dock preferences for the movie-editing workgroup to display only iMovie and the group folder. Because the group folder is in the Dock, it provides an easily accessible location for students to store and retrieve files.

Specifying No Group Folder

You can use Workgroup Manager to change a group account that has a group folder to one that has none. By default, a new group has no group folder.

To specify no group folder:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select an account, click the globe and choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Groups button and select a group.
5. Click Group Folder.
6. Select (None) in the list.

Creating a Group Folder

You can create a group folder for a group in any existing share point, or you can create the group folder in the /Groups folder—a predefined share point.

In Workgroup Manager, you can also create group folders that don't reside immediately below a share point. For example, you may want to organize group folders into several subfolders under a share point that you define. If Groups is the share point, you may want to place student groups' folders in /Groups/StudentGroups and teacher groups' folders in /Groups/TeacherGroups. The full path to a group folder for second-grade students could be /Groups/StudentGroups/SecondGrade.

Group folders are hosted on share points. For instructions on creating share points, see "Setting Up a Local Share Point" on page 104.

To set up a group folder in the /Groups folder or in another existing share point:

1. In Workgroup Manager, click Accounts.
2. Select the group account you want to work with.

   To select a group account, connect to the server where the account resides. Click the globe and choose the directory domain where the group account is stored, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Group Folder.
5. To add an existing share point to the list, click the Add (+) button and enter the requested information.

   In the URL field, enter the full URL to the share point where you want the group folder to reside. For example, enter "afp://myserver.example.com/SchoolGroups" to identify an AFP share point named "SchoolGroups" on a server whose DNS name is "myserver.example.com". If you are not using DNS, replace the DNS name of the server hosting the group folder with the server's IP address: "afp://192.168.2.1/SchoolGroups".

   In the Path field, enter the path from the share point to the group folder, including the group folder but excluding the share point. Do not put a slash at the beginning or the end of the path. For example, if the share point is SchoolGroups and the full path to the group folder is SchoolGroups/StudentGroups/SecondGrade, enter "StudentGroups/SecondGrade" in the Path field.

   Note: Configuring a group folder share point to have a network mount record does not make the group folder mount automatically when a group member logs in. You can provide easy access to a group folder by managing Dock preferences or Login preferences for the group.
6. In the Owner Name field, enter the name of the user you want to own the group folder so the user can act as group folder administrator.

   Click the Browse (...) button to choose an owner from a list of users in the current directory domain.

   The group folder owner is given read/write access to the group folder.
7. Click Save.
8. To create the folder, use the `ssh` tool to connect to the server hosting the share point and enter the `CreateGroupFolder` command in Terminal.

   You must be the root user to use the command. For more information about `ssh`, type `man ssh` in Terminal to see the man page. For more information about `CreateGroupFolder`, type `man CreateGroupFolder` in Terminal to see the man page.

   The group folder is named using the short name of the group with which it is associated.

You can automate a group member's access to the group folder when the user logs in:

- You can set up Dock Preferences to make the group folder visible in the Dock. For instructions, see "Providing Easy Access to Group Folders" on page 157.
- You can set up login preferences so that users can click Computer in the Finder to see the group folder share point and the group folders within it. For instructions, see "Providing Easy Access to the Group Share Point" on page 177.

When setting up these preferences, make sure the group is defined in a shared domain in the search policy of the group member's computer. See the Open Directory administration guide for instructions on setting a computer's search policy.

If you don't automate group folder access, group members can access the group folder using the "Connect to Server" command in the Finder's Go menu to navigate to the server where the group folder resides.

Designating a Group Folder for Use by Multiple Groups

To permit a group folder to be accessed by multiple groups, you identify the folder for each group separately.

To configure more than one group to use the same group folder:

1. In Workgroup Manager, click Accounts.
2. Select the first group account you want to use the folder.

   To select a group account, connect to the server where the account resides. Click the globe and choose the directory domain where the group account is stored, click the Groups button, and select the group.
3. Click Group Folder, select the folder you want the group to use, and click Save.
4. Repeat for each group you want to use the same group folder.

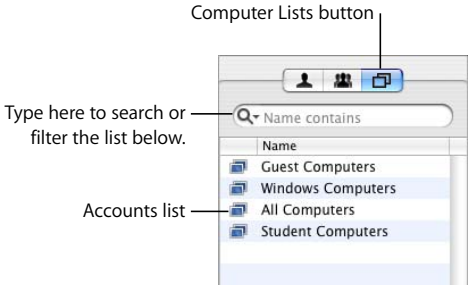
Setting Up Computer Lists

6

This chapter tells you how to set up and manage groups of computers.

When you want to manage a group of computers or restrict access to the group of computers to only certain groups of users, create a computer list for those computers.

You can use Workgroup Manager to view, create, edit, and delete computer lists. To view computer lists in Workgroup Manager, click the Computer Lists button above the accounts list.



About Computer Lists

A computer list comprises one or more computers that have the same preference settings and that are available to particular users and groups. You create and modify computer lists in Workgroup Manager.

There are three preexisting computer lists: Guest Computers, Windows Computers, and All Computers. These three lists, along with the computer lists that you set up, appear on the left side of the Workgroup Manager window. Settings appear in the List, Access, and Cache panes on the right side of the window.

Before you set up a computer list, determine the names and addresses of the computers that you want to include. In this context, you customarily use the computer name specified in a computer's Sharing preferences. If you prefer, you can use a descriptive name that you find more suitable.

A computer's address must be the built-in Ethernet address, which is unique to each computer. (A computer's Ethernet address, or Ethernet ID, is also known as its *MAC address*.) You can browse for a computer and Workgroup Manager enters the computer's name and Ethernet address for you. A client computer uses this data to find preference information when a user logs in.

Note: For Windows Computers lists, you need to know the NetBIOS name of each Windows client computer. This name is entered in the Windows Computer Name field. You don't need to know the Ethernet address of Windows client computers.

When a client computer starts up, Mac OS X tries to match the computer's Ethernet address with a computer record in a computer list. If a matching computer record is found, the computer uses the managed preferences for that computer list. If no matching computer record is found, the client computer uses the managed preferences for the Guest Computers computer list.

To edit computer lists or computer list preferences, you must have domain administrator privileges. You can have administrative privileges for all computer lists, or for a specific set of computer lists. For instructions on assigning administrator privileges for a directory domain, see "Assigning Administrator Privileges for a Directory Domain" on page 62.

Special Purpose Computer Lists

Workgroup Manager provides a default set of preexisting computer lists, each of which serves a special purpose. These lists are:

- *Guest Computers:* Computers that are not in any other list are automatically members of the Guest Computers list. You can inherit preferences for guest computers or define preferences for all guest computers.
- *Windows Computers:* A Windows Computers list is created automatically in the server's local directory and in the LDAP directory of an Open Directory master or replica. An administrator doesn't create and can't remove a Windows Computers list. For information and instructions on managing the Windows Computers list and on setting up Mac OS X Server as a primary or backup domain controller (PDC or BDC), see the Windows services administration guide.
- *All Computers:* This list holds all the computer records, whether present in a list or not. Computers that had previously been in lists can also be found here. This list serves as a handy reference location. You cannot manage preferences for this list.

Working with Guest Computers

If an unknown computer (one that isn't already in a computer list) connects to your network and attempts to access services, that computer is treated as a guest. Settings for the Guest Computers list apply to these unknown guest computers.

A Guest Computers list is automatically created for a server's local directory domain. If the server is an Open Directory master or replica, a Guest Computers list is also created for its LDAP directory domain.

The Guest Computers list is not recommended for large numbers of computers; most computers should belong to regular computer lists.

Note: You cannot add or move computers to the Guest Computers list, and you cannot change the list name.

To set up a Guest Computers list:

1. In Workgroup Manager, click Accounts.
2. Click the globe and choose the directory domain that contains the Guest Computers list you want to modify.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Computer Lists button (on the left) and select Guest Computers in the list.
5. Click List (on the right), and select a setting for preferences.

   If you want this Guest Computers list to get managed preference settings from the next directory domain in the directory server's authentication search policy, select "Inherit preferences for Guest Computers." For more information about search policies, see the Open Directory administration guide.

   If you want this Guest Computers list to have its own managed preference settings, select "Define Guest Computer preferences here."

   Important: To ensure that managed preference settings apply to mobile client computers while they're disconnected from the network, select "Define Guest Computer preferences here" or add the client computers to a specific computer list. Doing this caches managed preference settings on the client computers for offline use.
6. If you selected "Inherit preferences for Guest Computers," click Save.
7. If you selected "Define Guest Computer preferences here," click Access and select the settings you want to use. Click Cache, set an interval for clearing the preferences, and then click Save.

   After you set up the Guest Computers list, you can manage preferences for it if you wish. For more information about using managed preferences, see "Customizing the User Experience" on page 129 and Chapter 10, "Managing Preferences."

If you don't select settings or preferences for the Guest Computers list, guest computers are not managed. However, if the person using the guest computer has a Mac OS X Server user account with managed user or group preferences, those settings still apply when the person logs in with that user account.

Administering Computer Lists

This section describes how to administer computer lists stored in various kinds of directory domains.

Creating a Computer List

A computer list is a group of computers that have the same preference settings and that are available to the same users and groups. You can use a computer list to assign identical privileges and preferences to multiple computers. You can add up to 2000 computers to a computer list.

A computer cannot belong to more than one list, and you cannot add computers to the Guest Computers list.

To set up a computer list:

1. In Workgroup Manager, click Accounts.
2. Click the globe and choose the directory domain where you want to store the new computer list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Computer Lists button (on the left), and then click List (on the right).
5. To use a preset, choose one from the Presets pop-up menu.
6. Choose Server > New Computer List (or click New Computer List in the toolbar), and then type a name for the computer list.
7. To add a computer to the list, click the Add (+) button and enter the computer's Ethernet address and name. Or click the Browse (...) button and choose a computer, and Workgroup Manager enters the computer's Ethernet address and name for you.

   A computer's address must be the unique built-in Ethernet address, even if the client is connected to the network using AirPort. (A computer's Ethernet address, or Ethernet ID, is also known as its *MAC address*.) If you manually add a computer, be sure to use the built-in Ethernet address for each client.
8. Optionally, add a comment.

   Comments are useful for providing 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 identification information such as the computer's model or serial number.

9 Continue adding computers until your computer list is complete.

10 Fill in the information requested in the Access and Cache panes.

11 Save the computer list.

After you set up a computer list, you can manage preferences for it if you wish.

For more information about using managed preferences, see "Customizing the User Experience" on page 129 and Chapter 10, "Managing Preferences."

Creating a Preset for Computer Lists

You can select settings for a computer list and save them as a "preset." Presets work like templates, allowing you to apply preselected settings and information to new computer lists. Using presets, you can easily set up multiple computers to use similar settings. You can use presets only when creating a new computer list; you can't use a preset to modify an existing computer list.

Settings in the List pane are specific to individual computers, and don't apply to presets.

To set up a preset for computer lists:

1 In Workgroup Manager, click Accounts.

2 Click the globe and choose the directory domain where you want to create a computer list using presets.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Click the Computer Lists button (on the left), and then click List (on the right).

5 To create a completely new preset, first create a computer list by clicking New Computer List. To create a preset using data in an existing computer list, select it (on the left).

6 Fill in the information requested in the Access and Cache panes.

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 change its name or delete it. To change a preset's name, choose the preset from the Presets pop-up menu, and then choose Rename Preset. To delete a preset, choose a it from the Presets pop-up menu, and then choose Delete Preset.

Using a Computer List Preset

When you create a new computer list, you can choose any preset from the Presets pop-up menu to apply initial settings; you can further modify the computer list settings before you save the list. When you save the computer list, you can't use the Preset menu again for that list (for example, you can't apply a different preset to the list).

To use a preset for computer lists:

1. In Workgroup Manager, click Accounts.
2. Click the globe and choose the directory domain where you want to store the new list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Computer Lists button (on the left), and then click List (on the right).
5. Choose a preset from the Presets pop-up menu.
6. Create a new list (click New Computer List).
7. Add or update settings as needed, and then save the list.

Adding Computers to an Existing Computer List

You can easily add more computers to an existing list. You can't add computers to the Guest Computers list, however, because it is predefined to include just the computers that are not part of another computer list.

To add computers to a list:

1. In Workgroup Manager, click Accounts.
2. Select the computer list.

   To select the list, click the globe and choose the directory domain that contains the list, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click List.
5. Click the Add (+) button and enter the requested information.

   Or click the Browse (...) button, select the computer you want, and Workgroup Manager enters the computer's Ethernet address and name for you.

   A computer's address must be the built-in Ethernet address, which is unique to each computer. (A computer's Ethernet address, or Ethernet ID, is also known as its *MAC address*.)
6. Optionally, add 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 identification information such as the computer's model or serial number.
7. Click Save.
8. Continue adding computers and information until your list is complete.

Changing Information About a Computer

After you add a computer to a computer list, you can edit information whenever necessary.

To change computer information:

1. In Workgroup Manager, click Accounts.
2. Select the list to which the computer belongs.

   To select the list, click the globe and choose the directory domain that contains the computer you want to modify, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the List pane, select the computer whose information you want to edit and click the Edit (pencil) button.

   Or double-click the Address, Description, or Comment field of a computer in the list to edit the information directly in the list.
5. Change information as needed, and then click Save.

Moving a Computer to a Different Computer List

If you ever need to group computers differently, you can easily move computers from one list to another.

Note: A computer can belong to only one list. You can't add computers to the Guest Computers list.

To move a computer from one list to another:

1. In Workgroup Manager, click Accounts.
2. Select the list to which the computer belongs.

   To select the list, click the globe and choose the directory domain that contains the computer list you want to modify, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the List pane, select the computer you want to move and click the Edit (pencil) button.
5. Choose a list from the Computer List pop-up menu and click OK.
6. Click Save.

Removing Computers from a Computer List

After you delete a computer from a computer list, that computer is managed from the Guest Computers list.

To remove a computer from a list:

1. In Workgroup Manager, click Accounts.
2. Select the list to which the computer belongs.

   To select the list, click the globe and choose the directory domain that contains the computer list you want to modify, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. In the List pane, select one or more computers.
5. Click the Remove (–) button, and then click Save.

Deleting a Computer List

If you no longer need any computers to be in a computer list, you can delete the entire list. You can't delete the Guest Computers list or the Windows Computers list.

> *Warning:* You can't undo this action.

To delete a computer list:

1. In Workgroup Manager, click Accounts.
2. Select the list.

   To select the list, click the globe and choose the directory domain that contains the computer list you want to delete, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Choose Server > Delete Selected Computer List, or click Delete in the toolbar.

Searching for Computer Lists

Workgroup Manager has a search feature that allows you to find specific computer lists quickly. You can search within a selected domain and filter the search results.

To search for a computer list:

1. In Workgroup Manager, click Accounts, click the Computer Lists button (on the left), and then click List (on the right).
2. To limit your search, click the globe and choose a directory domain:

   Local: Search for computer lists in the local directory domain.

   Search Path: Search for computer lists in all directories of the server's search policy (for example, myserver.mydomain.com).

   Other: Browse and select an available directory domain to search for computer lists.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 Select an additional filter from the filter pop-up menu next to the search field, if you wish.

5 Type search terms in the search field.

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 restrict access to computers so that only certain users have access to them. For example, if you have two computers with video-editing hardware and software, you can reserve them for users doing video production. First, create a computer list of those computers, make sure the users have user accounts, add the users to a "video production" group, and then give only that group access to the video-production computer list. The "video production" group will then be able to access the computers in the computer list.

Note: A user with an administrator account in a client computer's local directory can always log in.

To reserve a set of computers for specific groups:

1 In Workgroup Manager, click Accounts.

2 Select the computer list.

To select the list, click the globe and choose the directory domain that contains the computer list, click the Computer Lists button, and select the list.

3 To authenticate, click the lock and enter the name and password of a directory domain administrator.

4 In the List pane, enter the computer records with their Ethernet IDs.

5 Click Access.

6 Select "Restrict to groups below."

7 Click the Add (+) button, and then select one or more groups in the drawer and drag them to the list in the Access pane.

To remove an allowed group, select it and click the Remove (–) button.

8 Click Save.

Only users of the permitted groups are displayed in the login window and can log in.

Making Computers Available to All Users

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. In Workgroup Manager, click Accounts.
2. Select the computer list.

   To select the list, click the globe and choose the directory domain that contains the computer list, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click the Computer Lists button and select one or more computer lists.
5. In the List pane, check the computer records or enter one if none exists.
6. Click the Access pane.
7. Select "All groups can use the computer" and "Allow computer administrators to disable management."
8. Click the Cache pane and ensure that the setting for updating the preference cache is set to the appropriate duration.

   > *Warning:* Do not set the cache refresh to "0." This would prevent the creation of the cache and result in the computers becoming unmanaged when disconnected from the network.

9. Click Save.

Using Local User Accounts

A *local user account* is a user account defined in a client computer's local directory domain. 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 each 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 decide not to be managed.

The easiest way to manage preferences for local users of a particular computer is to manage preferences for the computer list to which the computer belongs, and make sure you allow users with local-only accounts to use computers in the computer list.

To provide access for users with local accounts:

1. In Workgroup Manager, click Accounts.
2. Select a computer list that supports computers with local users.

   To select a list, click the globe and choose the directory domain that contains the computer list, click the Computer Lists button, and select the list.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Access.
5. Select "Restrict to groups below" to determine which workgroups are displayed when a local user logs in. Drag groups from the drawer to the list in the Access pane.

   If you select "All groups can use the computer," users log in without having to select a workgroup.
6. If you selected "Restrict to groups below," select "Local-only accounts pick workgroups from the above list," to require that users select one of those workgroups.

   The workgroup picker is only displayed if client computers use Mac OS X version 10.4 or later. Additionally, if there is only one workgroup, the user will automatically log in as a member of that workgroup.

   If you do not select "Local-only accounts pick workgroups from the above list," local users do not have to select a workgroup.
7. Make sure "Allow users with local-only accounts" is selected.
8. Click Save.

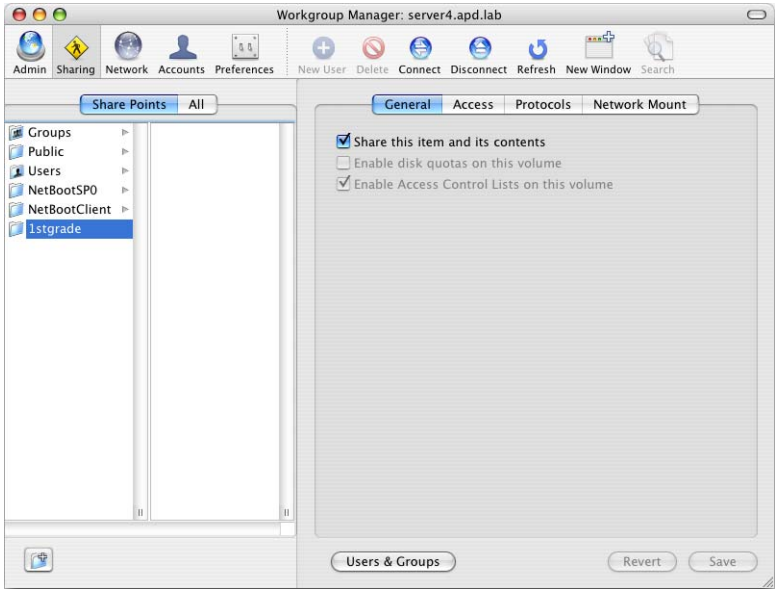
Setting Up Home Folders

7

This chapter provides guidelines for setting up and managing home folders.

Mac OS X uses the home folder—a folder for a user's personal use—to store the user's application preferences and personal files like documents and music.

You can use the Sharing pane in Workgroup Manager to configure folders for use as home folder locations.



About Home Folders

You can set up home folders so they can be accessed using Apple Filing Protocol (AFP), Network File System (NFS), or Server Message Block/Common Internet File System (SMB/CIFS).

To set up a home folder for a user in Workgroup Manager, you use the Home pane in the Accounts window.

You can also import user home folder settings from a file. For an explanation of how to work with import files, see Appendix A, "Importing and Exporting Account Information."

A user's home folder doesn't need to be stored on the same server as the directory domain containing the user's account. In fact, distributing directory domains and home folders among various servers can help you balance your workload among several servers. "Distributing Home Folders Across Multiple Servers" on page 103 describes several such scenarios.

The home folder that you designate in the Home pane can be used when logging in from a Windows workstation or a Mac OS X computer. This can be useful for a user whose account resides on a server that is a Windows primary domain controller. See the Windows services administration guide for information about setting up home folders for Windows workstation users.

> ***Warning:*** If the absolute path from the client to the network home folder on the server contains either spaces or more than 89 characters, certain types of clients cannot connect. For example, a client using automount with an LDAP-based AFP home folder may not be able to access its home folder. The "/" character counts as a character.

There are additional limitations on the maximum path length depending on the version of Mac OS X used by clients. For more information, see the Apple Service & Support website article "Avoid Spaces and Long Names in Network Home Directory Name, Path" at docs.info.apple.com/article.html?artnum=107695.

Hosting Home Folders for Mac OS X Clients

To host home folders for Mac OS X clients, it is recommended that you use AFP or NFS. If you are hosting only Mac OS X clients, use AFP. If you are hosting both Mac OS X and UNIX clients, use 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.

NFS file access is based not on user authentication, but on the user ID and the client IP address, so it is generally less secure than AFP. Use NFS only if you need to provide home folders for a large number of users who use UNIX workstations.

Hosting Home Folders for Other Clients

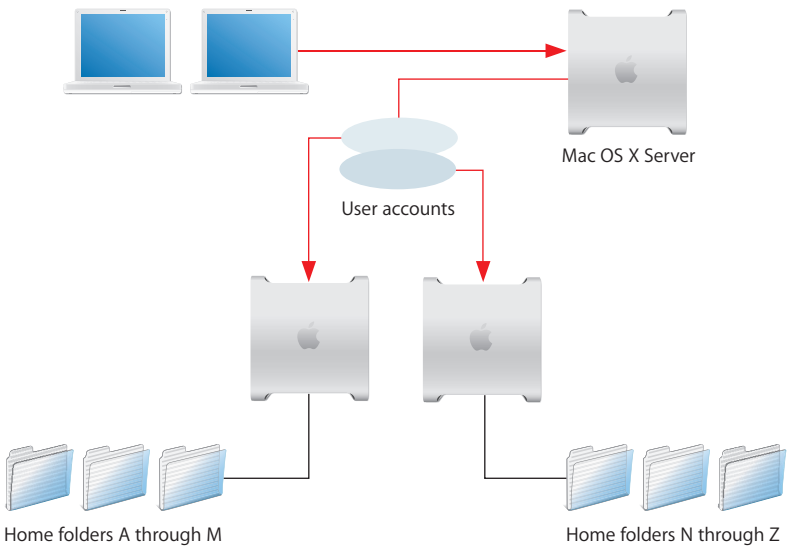
To host home folders for Windows clients, use SMB/CIFS. To optimally handle both Mac OS X and Windows clients, you could use both AFP (for the Mac OS X clients) and SMB/CIFS (for the Windows clients).

SMB/CIFS is a protocol used by Windows to access share points. You can setup a share point for SMB/CIFS access only, so that Windows users have a network location for files that can't be used on other platforms. Like AFP, SMB/CIFS also requires authenticating with a valid name and password to access files.

For more details about the SMB/CIFS protocol, including information about setting up SMB/CIFS share points for hosting home folders, see the Windows services administration guide.

Distributing Home Folders Across Multiple Servers

The following illustration depicts using one Mac OS X Server computer for storing user accounts and two other Mac OS X Server computers for storing AFP home folders.



When a user logs in, he or she is authenticated using an account stored in a shared directory domain on the accounts server. The location of the user's home folder, stored in the account, is used to mount the home folder, which resides on one of the two home folder servers.

Here are the steps you could use to set up this scenario for AFP home folders:

Step 1: Create a shared domain for the user accounts on the accounts server
You create a shared LDAP directory domain by setting up an Open Directory master, as described in the Open Directory administration guide.

Step 2: Set up an automountable share point for the home folders on each home folder server
For instructions on how to set up automountable share points, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 105.

Step 3: Create the user accounts in the shared domain on the accounts server
Instructions later in this chapter explain how to set up accounts so that home folders reside in one or the other of the automountable share points.

See the instructions in "Creating Mac OS X Server User Accounts" on page 51 to learn how to set user account attributes. See subsequent sections of this chapter for details specific to home folder setup.

Step 4: Set up the directory services of the client computers so their search policy includes the shared directory domain on the accounts server
See the Open Directory administration guide for information about configuring search policies.

When a user restarts his or her computer and logs in using the account in the shared domain, the home folder is created automatically (if it hasn't already been created) on the appropriate server and is visible on the user's computer.

Administering Share Points

A share point is a hard disk (or hard disk partition), CD-ROM disc, or folder that contains files you want users to share. You can use share points to host home folders.

Setting Up a Local Share Point

You can use Workgroup Manager to set up a local share point. You can then use this share point to host local home folders, or you can mount the share point so that it can host network home folders.

To set up a local share point:

1 On the server where you want the share point to reside, create a folder that will serve as the share point.

If you are planning on using this share point for home folders, you may want to set up home folder share points on a partition different from other share points. See "Setting Disk Quotas" on page 113 for more information.

2 Open Workgroup Manager, connect to the server that hosts the share point, and click Sharing.

To connect to the server, open the Workgroup Manager Connect window by choosing Server > Connect. Enter the server address in the Address field.

3 Click All (above the list on the left) and select the folder you created for the share point.

4 In the General pane, select "Share this item and its contents."

5 Click Access and specify the share point owner and group names by typing names into those fields or by dragging names from the drawer that opens when you click Users & Groups. Enter "admin" in the Owner field.

Entering "admin" in the owner field secures the share point from other users getting write access and prevents them from moving or deleting home folders.

6 Set Owner permissions to Read & Write, and set Group permissions and Everyone permissions to Read Only.

7 Click Save.

Setting Up an Automountable AFP Share Point for Home Folders

You can use Workgroup Manager to set up an AFP share point for home folders.

Home folders for user accounts stored in shared directory domains, such as the LDAP directory of an Open Directory master, can reside in any AFP share point that the user's computer can access. This share point must be automountable—that is, it must have a network mount record in the directory domain where the user account resides.

Using an automountable share point ensures that the home folder appears in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain. Additionally, users can access home folders on any automountable share point with guest access enabled.

To set up an automountable AFP share point for home folders:

1 If you do not already have a share point that you would like to host home folders on, create one. For instructions, see "Setting Up a Local Share Point" on page 104.

2 Open Workgroup Manager, connect to the server that hosts the share point, and click Sharing.

To connect to the server, open the Workgroup Manager Connect window by choosing Server > Connect. Enter the server address in the Address field.

3 Click Share Points (above the list on the left) and select the share point.

4 Click Network Mount and authenticate as an administrator of the directory domain in which the user account resides.

Use the Where pop-up menu to choose the directory domain where the user account resides. Then click the lock and authenticate as an administrator of the directory domain.

5 Select "Enable network mounting of this share point" and "Use For User Home Directories."

6 Make sure the Protocol pop-up menu is set to AFP, and click Save.

7 Set up guest access to the share point.

Click Protocols, choose Apple File Settings from the pop-up menu, and make sure "Share this item using AFP" and "Allow AFP guest access" are selected.

In Server Admin, make sure AFP guest access is enabled. Connect to the home folder server and select AFP in the Computers & Services list. Click Settings, and then click Access, and make sure "Enable Guest access" is selected. Also make sure the AFP service is running.

When you enable guest access for a share point, it automatically enables guest access for all home folders located in the share point. By default, within home folders, guests can only access the /Public and /Sites folders. When a guest browses the home folder server, they can see who has home folders on that server but are restricted to opening guest access–enabled folders. In addition to browsing the home folder server, guests can also use ~*user-short-name*/Public to access a user's /Public folder.

Setting Up an Automountable NFS Share Point for Home Folders

Although AFP is the preferred protocol for accessing home folders because of the security it offers, you can use Workgroup Manager to set up a network NFS share point for home folders. NFS share points can be used for home folders of users defined in shared directory domains, such as the LDAP directory of an Open Directory master or an Active Directory domain. The NFS share point must be automountable—that is, it must have a network mount record in the directory domain where the user account resides.

An automountable share point ensures that the client computer can locate the NFS share point and the home folder. It also makes the share point's server visible in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain.

To set up an automountable NFS share point for home folders:

1 If you do not already have a share point that you would like to host home folders on, create one. For instructions, see "Setting Up a Local Share Point" on page 104.

2 Open Workgroup Manager, connect to the server that hosts the share point, and click Sharing.

To connect to the server, open the Workgroup Manager Connect window by choosing Server > Connect. Enter the address of the server in the Address field.

3 Click Share Points (above the list on the left) and select the share point.

4 Click Protocols, and then choose NFS Export Settings from the pop-up menu.

5 Select "Export this item and its contents to" and make sure Client is chosen in the pop-up menu below it.

6 Add client computers that you want to be able to access the share point.

Click Add and type the IP address or host name of a client you want to add to the Computer list.

Click Remove to remove the selected client computer from the list.

7 Set up share point permissions.

Select "Map Root user to nobody" and deselect the remaining boxes.

8 Click Network Mount and click the lock to authenticate as an administrator of the directory domain where the user account resides.

Use the Where pop-up menu to choose the directory domain where the user account resides. Then click the lock and authenticate as an administrator of the directory domain.

9 Select "Enable mounting of this share point" and "Use For User Home Directories."

10 Choose NFS from the Protocol pop-up menu and click Save.

Administering Home Folders

You can use Workgroup Manager to assign a home folder location to user accounts. In order to assign a home folder location, you first need to create a share point. For instructions on creating share points, see "Setting Up a Local Share Point" on page 104.

Specifying No Home Folder

You can use Workgroup Manager to change a user account that has a home folder to one that has none. By default, new users have no home folder. When users do not have home folders, they cannot save files locally.

> ***Warning:*** Portable home directories require specifying a network home folder.

To define no home folder:

1 In Workgroup Manager, click Accounts.

2 Open the directory domain where the user account resides and authenticate as an administrator of the domain.

To open a directory domain, click the globe and choose from the pop-up menu. To authenticate, click the lock.

3 Click the Users button and select one or more user accounts.

4 Click Home, and then select (None) in the list.

5 Click Save.

Creating a Home Folder for a Local User

You can use Workgroup Manager to define home folders for users whose accounts are stored in a server's local directory domain. You might want to use local user accounts on standalone servers (servers not accessible from a network) and for administrator accounts on a server. These accounts are meant to be used by users logging in to the server locally. They are not meant to be used by network users.

Home folders for local users should reside in share points on the server where the users' accounts reside. These share points do not have to be automountable (that is, they do not require a network mount record).

To create a home folder for a local user account:

1 If you do not already have a share point for local user account home folders, create one. For instructions, see "Setting Up a Local Share Point" on page 104.

2 Open Workgroup Manager and click Sharing.

3 Click All (above the list on the left) and select the folder you created for the share point.

4 In Workgroup Manager, click Accounts and select the user account you want to work with.

To select a local user account, click the globe and choose the local directory domain, click the Users button, and then select the user account in the accounts list.

5 Click the lock and authenticate as an administrator of the local directory domain.

6 Click Home to set up the selected user's home folder.

7 In the share points list, select the share point you want to use.

The list displays all the share points on the server you are connected to.

8 Optionally, enter a disk quota and specify megabytes (MB) or gigabytes (GB).

9 Click Create Home Now, and then click Save.

If you do not click Create Home Now before clicking Save, the home folder is created the next time the user logs in remotely. However, only certain clients can connect to servers hosting share points in the local domain. For instructions on setting up a share point for Mac OS X clients, see "Creating a Network Home Folder" on page 109.

The home folder has the same name as the user's first short name.

Creating a Network Home Folder

In Workgroup Manager, you can set up a network home folder for a user account stored in a shared directory domain.

A user's network home folder can reside in any AFP, NFS, or SMB/CIFS share point that the user's computer can access. Mac OS X home folders typically reside in AFP or NFS share points, while Windows home folders typically reside in SMB/CIFS share points.

For information about how to set up SMB/CIFS share points for Windows user home folders, see the Windows services administration guide.

The share point must be automountable—that is, it must have a network mount record in the directory domain. An automountable share point ensures that the client computer can locate the share point and the home folder. It also makes the share point's server visible in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain.

You can use Workgroup Manager to define a network home folder for a user whose account is stored in the LDAP directory of an Open Directory master or another read/write directory domain accessible from the server you are using. You can also use Workgroup Manager to review home folder information in any accessible read-only directory domain.

To create a network home folder in an AFP or NFS share point:

1. Make sure that the share point exists on the server where you want the home folder to reside, and that the share point has a network mount record configured for home folders.

   For instructions, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 105, or "Setting Up an Automountable NFS Share Point for Home Folders" on page 106.

2. In Workgroup Manager, click Accounts and select the user account you want to work with.

   To select an account, connect to the server where the account resides. Click the globe and choose the directory domain where the user account is stored. Click the Users button and select the user account in the accounts list.

3. To authenticate, click the lock and enter the name and password of a directory domain administrator.

4. Click Home to set up the selected user's home folder.

5. In the share points list, select the share point you want to use.

The list displays all the automountable network-visible share points in the search policy of the server you are connected to, as well as custom home folder locations in the directory domain. If the share point you want to select is not listed, try clicking Refresh. If the share point still does not appear, it might not be automountable. In this case, you need to set up the share point to have a network mount record configured for home folders as described in step 1, or create a custom home folder location as described in "Creating a Custom Location for Home Folders" on page 110.

6 Optionally, enter a disk quota and specify megabytes (MB) or gigabytes (GB).

7 Click Create Home Now, and then click Save.

For AFP share points, if you do not click Create Home Now before clicking Save, the home folder is created the next time the user logs in remotely. For NFS share points, you are required to click Create Home Now before clicking Save.

The home folder has the same name as the user's first short name.

8 If the home folder is in a new NFS share point, make sure that the user restarts his or her client computer so that the share point is visible on it.

When the user logs in using SSH to obtain command-line access to the server, the user's home folder is mounted.

Creating a Custom Location for Home Folders

The user's home folder does not have to reside in the share point folder. For example, you can organize home folder locations by creating several subfolders within a share point. If /Homes is the share point folder, you can place teacher home folders in /Homes/Teachers and student home folders in /Homes/Students.

You can use Workgroup Manager to define a custom location for the home folder of a user whose account is stored in a server's local directory domain or in a shared directory domain. The shared directory domain must be accessible from the server that you are using. The shared directory domain can be the LDAP directory of an Open Directory master, or another read/write directory domain.

Important: The procedure described here requires Mac OS X Server version 10.4.3 or later.

To create a custom home folder using Workgroup Manager:

1 Make sure the share point exists and is configured correctly.

The share point for a local user account's home folder should reside in an AFP share point on the server where the user account resides. This share point does not have to be automountable—that is, it does not require a network mount record in the directory domain.

The share point for the home folder of a user account in a shared directory domain can reside in any share point that the user's computer can access. This share point must be automountable. Additionally, any NFS share point used for home folders must be automountable.

For instructions on setting up AFP or NFS share points for home folders, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 105 or "Setting Up an Automountable NFS Share Point for Home Folders" on page 106. For instructions on setting up SMB/CIFS share points for home folders, see the Windows services administration guide.

2 If you want the home folder to reside beneath a folder under the share point, you can use Workgroup Manager or Finder to create all the folders in the path between the share point and where the home folder will reside.

3 In Workgroup Manager, click Accounts and select the user account you want to work with.

To select an account, connect to the server where the account resides. Click the globe and choose the directory domain where the user account is stored. Click the Users button and select the user account.

4 To authenticate, click the lock and enter the name and password of a directory domain administrator.

5 Click Home to set up the selected user's home folder.

6 Click the Add (+) button to add a custom home folder location, or click the Duplicate (copy icon) button to copy an existing location.

You can remove a home folder location by selecting it and clicking the Delete (–) button. You can delete only the locations that were added with the Add or Duplicate buttons.

7 In the Mac OS X Server/Share Point URL field, either enter the full URL to an existing automountable AFP share point where you want the home folder to reside, or leave this field blank for an NFS share point.

For example, if the AFP share point is /Homes and you are using DNS, you might enter "afp://server.example.com/Homes." If you are not using DNS, replace the DNS name of the server hosting the home folder with the server's IP address: afp://192.168.2.1/Homes." Don't put a slash (/) at the end of the URL.

8 In the Path field, enter the path from the AFP share point to the home folder, including the home folder but excluding the share point; leave this field blank for an NFS share point.

For example, to create a home folder for a user named Smith, located in a custom location of /Homes/Teachers/SecondGrade/, enter "Teachers/SecondGrade/Smith". Make sure that the custom location folder exists.

Do not put a slash at the beginning or the end of the path.

9 In the Home field, enter the full path to the home folder, ending with the home folder itself. Note that this field automatically updates whenever you change entries in the Mac OS X Server/Share Point URL or Path fields.

In the Home field, enter a location in this format:

[/Network/Servers/*server's-host-name/*][Volumes/[*drive/*]*volume/*]*share-point/path*

The entries within brackets ([]) are optional. Include them only if they apply to the particular share point location. If the share point is for local user accounts, do not include /Network/Servers/server's-host-name.

Replace the following elements:

- *server's-host-name*: Replace this with the AFP server's host name.
- *drive*: If the share point is stored on a server with multiple storage devices, replace this with the name of the storage device.
- *volume*: If the share point is stored on a server with multiple volumes, replace this with the name of the volume storing the share point.
- *share-point*: Replace this with the name of the share point.
- *path*: Replace this with the path you entered in the previous step.

Use an initial slash (/) but no terminating slash.

For example, the following is a Home entry for a custom home folder for local users:
/Homes/Teachers/SecondGrade/Smith

The following is a Home entry for a custom home folder in the HardDrive volume stored in a server located at server.example.com:
/Network/Servers/server.example.com/Volumes/HardDrive/Homes/Teachers/SecondGrade/Smith

If you used a volume named HomeFolders in an external drive named externalHD as a location for a custom home folder, the Home entry looks like this:

/Network/Servers/server.example.com/Volumes/externalHD/HomeFolders/Homes/Teachers/SecondGrade/Smith

10 Click OK.

11 Optionally, enter a disk quota and specify megabytes (MB) or gigabytes (GB).

12 Click Create Home Now, and then click Save.

If you do not click Create Home Now before clicking Save, the home folder is created the next time the user logs in to a client computer.

Note: Home folders are automatically created the first time a user logs in only on share points served via an AFP or SMB/CIFS server. NFS home folders must be created manually.

Setting Disk Quotas

You can limit the disk space users can use to store files in the partition where their home folders resides.

This quota doesn't apply to the home folder share point or to the home folder, but to the entire partition within which the home folder share point and the home folder reside. Therefore, when a user places files in another user's folder, it can affect 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 folder share point disk quota using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to work with.

   To select an account, connect to the server where the account resides, click the globe and choose the directory domain where the user account is stored, click the Users button, and select the user account.
3. To authenticate, click the lock and enter the name and password of a directory domain administrator.
4. Click Home.
5. Specify the disk quota using the Disk Quota field and the adjacent pop-up menu.
6. Make sure that disk quotas are enabled for the volume where the share point resides.
7. Click Sharing, and select the volume in the All list. Click General and choose "Enable disk quotas on this volume."

Choosing Default Home Folders by Using Presets

You can define default home folder settings to use for new users by using a preset to predefine them. For information about defining and using presets, see "Using Presets to Create New Accounts" on page 55.

Moving Home Folders

If you need to move a home folder, create the new home folder and copy the contents of the old home folder into the new home folder before deleting the old home folder.

Deleting Home Folders

When you delete a user account, the associated home folder is not automatically deleted. The administrator must delete the home folder manually by moving it to Trash.

User Management for Portable Computers

8

This chapter provides information about the tools available to facilitate the management of portable computers.

With Mac OS X Server, you can create and manage mobile accounts. These accounts are designed for the users of portable computers.

About Mobile Accounts

If you distribute portable computers, you can give mobile accounts to users so that you can manage their preferences and control their level of access to local and network resources. These mobile accounts, which are specially designed for portable computers, provide many advantages over using local or network accounts.

A mobile account includes both a network home folder and a local home folder. By having these two types of home folders, clients can take advantage of features available for both local and network accounts. You can synchronize specific folders of these two home folders, creating a portable home directory.

Synchronization ensures that users access their most recently updated files whenever they connect to the network. If a user modifies files on different computers, when the user connects to the network and synchronizes, the user's computer retrieves the most recently synchronized file.

Mobile accounts also cache authentication information and managed preferences. A user's authentication information is maintained on the directory server, but cached on the local computer. With cached authentication information, a user can log in using the same user name and password, even if he or she is not connected to the network. For example, when a student has a mobile account, the student's login name, password, and preferences defined for the user account, workgroups, and computer are the same at school and at home. If you change any of these items, the local versions are updated the next time the user logs in at school.

About Portable Home Directories

Portable home directories are a new feature of Mac OS X version 10.4. A portable home directory is a synchronized subset of a user's local and network home folders.

You can configure which folders to synchronize and how often to synchronize them. Users can also initiate synchronization. By synchronizing key folders, a user can work on or off the network and experience the same work environment. Since the user has a local home folder, and only synchronizes periodically or at login and logout, the mobile account reduces network traffic, expediting server connections for users who need to access the server. Additionally, the computer locally caches temporary files. This improves both network and individual computer performance because the user's computers locally caches files like web pages.

In Mac OS X version 10.3, mobile accounts did not synchronize local and network home folders. Before the introduction of synchronization, portable home directories did not exist. When you manage clients with Mac OS X version 10.3 installed, you can still give them mobile accounts but they do not have synchronized home folders.

Users with accounts stored in an Active Directory domain can have mobile accounts. Similar to mobile accounts for clients with Mac OS X version 10.3 installed, these mobile accounts do not synchronize. Instead of synchronization, users must manually copy files from their local home folders to their network home folders.

There are two ways to create mobile accounts: you use Workgroup Manager to enable synchronization of user accounts, or let network users create mobile accounts themselves. For instructions on using Workgroup Manager to enable synchronization, see "Creating a Mobile Account" on page 186.

Users with network accounts who also have administrative access to their computers can create mobile accounts, which creates a portable home directory. Because they create the mobile accounts themselves, you do not have control over their synchronization settings, unless you explicitly manage their mobile accounts. If you want to prevent them from creating mobile accounts, you can choose not to show Accounts in their System Preferences. For instructions on denying access to specific System Preferences, see "Managing Access to System Preferences" on page 197. You can also manage their Mobility preferences so that users cannot create mobile accounts. For instructions on managing Mobility preferences, see "Preventing the Creation of a Mobile Account" on page 187.

Logging In to Mobile Accounts

If a user has previously created a portable home directory, logging in to a mobile account is very similar to logging in to a local account.

If a computer is configured to display a list of only the users with local accounts at login, only the users with mobile accounts who have created portable home directories are displayed. If the user does not create a portable home directory for the local computer, a mobile account is treated like a network account.

At the login window, the user with a mobile account selects his or her account and then enters the correct password to complete login. If the user already has a mobile account with a portable home directory, his or her folders might get synchronized depending on the login and logout synchronization settings set in Workgroup Manager. After this, the user's desktop appears.

If the user does not have a mobile account with a portable home directory, one of two things occur:

- If you deselected "Require confirmation before creating a mobile account," the computer automatically creates the mobile account. The local home folder then synchronizes with the user's network home folder before displaying the user's desktop.
- If you selected "Require confirmation before creating a mobile account," the user sees a confirmation dialog that allows them to create a portable home directory, put it off until later, or not create the portable home directory and disable the dialog until the user holds down the Option key during login.

Mobile accounts remain on the system even when the user logs out or disconnects from the network. Even when disconnected, the user can log in to that account.

Considerations and Strategies for Deploying Mobile Accounts

When you properly configure mobile accounts, you can create a work environment where users effortlessly access their latest files from several locations, keep their managed preferences while offline and can retrieve file backups if users lose or damage their computers, all while requiring less network traffic than network accounts. When improperly configured, mobile accounts can overload the server, force users to wait for a long period of time to log in or log out, and could cripple client computers by using up all available hard disk space.

Carefully weigh the advantages and disadvantages of using mobile accounts and strategize how you will configure them.

Advantages of Using Mobile Accounts

Mobile accounts have several advantages over using either local or network accounts:

- **Applications locally cache temporary files.**

  When mobile account users run applications, those applications cache temporary files on the local computer. When network account users run applications, instead of caching, those applications transfer temporary files over the network.

In addition to the speed increase gained by not having to repeatedly transfer temporary files, using mobile accounts can also improve application stability. Some applications are not designed to work with network home folders and non–locally cached temporary files. By using mobile accounts, these applications run as though the user had a local account.

- **Mobile accounts can create less network traffic than network accounts.**

  When network account users save files, they transfer the files over the network. When they open files, they also transfer files over the network. With a mobile account, files are stored locally and are only transferred during synchronization. Synchronization only transfers files if the local and network files have mismatched modification times, in which case the newer file takes precedence.

  Mobile accounts cache temporary files locally, improving both network and individual computer performance. Caching files like web pages locally helps reduce network traffic.

  You can also reduce network traffic by planning users' synchronization settings carefully. For information about how to plan synchronization settings, see "Strategies for Synchronizing Content" on page 120.

- **You can manage individual mobile accounts.**

  Like network accounts, you can use Workgroup Manager to manage preferences and set account attributes for individual mobile accounts.

  You can manage users with local accounts only if you add a computer to a computer list. This allows you to set management preferences affecting all local accounts for that computer, but it doesn't let you manage individual local accounts. To manage specific local accounts, you would have to log in to the local computers individually, or use Apple Remote Desktop.

- **Users can access their accounts and files when disconnected from the network.**

  Mobile accounts have two key features that allow users to access their accounts and files when disconnected from the network: cached authentication and portable home directories.

  With cached authentication, when mobile account users disconnect from the network, the user can log in to the portable computer using the same login name and password as they did when the computer was last connected. By contrast, network account users cannot access their accounts when they disconnect from the network. If you change the password for a user remotely, the next time he or she connects to the network, he or she has to use the new password to authenticate.

  For information about portable home directories, see "About Portable Home Directories" on page 116.

- **Users can recover their data if their computers are lost or damaged.**

  If a user with a mobile account loses or damages his or her portable computer and logs in using a new computer, the server restores all previously synchronized files during the next synchronization.

Disadvantages of Using Mobile Accounts

Although mobile accounts provide many advantages over local and network accounts, they also have a few disadvantages:

- **Improperly set synchronization settings can cause long delays at login and logout, or create inconsistent home folders.**

  If you synchronize large files only at login and logout, this could substantially delay your users' login and logout. If they make changes to large files, they have to wait for the files to synchronize before they can finish logging in or logging out. If many users who make changes to large files log in to a wireless network with limited bandwidth simultaneously, they can overload the network, further delaying their login.

  If you do not synchronize key folders, this can create inconsistent home folders and confuse your users. For example, say you are a school administrator and you only synchronize a student's ~/Documents folder. If students don't save their homework in the ~/Documents folder, they cannot access their homework using their mobile account on another computer. Also, if homework saved in ~/Documents references pictures located in ~/Pictures, the references might not work because the ~/Pictures folder is not synchronized.

- **If multiple users create a mobile account on the same computer, they could cause excessive home folder proliferation.**

  If you have a shared-access computer like a kiosk or a lab computer, every time a user creates his or her mobile account, the user creates a local home folder. If unmanaged, this could completely fill the available hard disk space of the computer. In this case, you would want to use either network or generic local accounts, both of which stop the user from creating local home folders. If you still want to use mobile accounts, you may want to write a logout script or a script you run using Apple Remote Desktop to prevent home folder proliferation.

- **Synchronizing large home folders or packages can negatively impact server performance.**

  Synchronizing more than a gigabyte of files can negatively impact server performance because the server must compare the last modification date of each file. Comparing a large number of files for multiple users simultaneously can overburden the server. Your server then becomes backlogged, slowing performance for other users.

Synchronizing packages—single files that represent a hidden folder structure with files—can also overload the server. By synchronizing a package, you're effectively synchronizing each one of those hidden files and folders. If users want to synchronize packages, consider asking them to archive packages to single files so that they don't synchronize hidden files and folders.

Make sure that you synchronize only key folders, and that you do not synchronize unnecessary folders. Consider using a disk quota per user to limit the amount of content they can store and synchronize.

- **Mobile accounts cannot restore deleted files through synchronization.**

  Although mobile accounts keep your users' files stored in two locations—in local and network home folders—they do not eliminate the need for a formal backup system. When you configure the user's portable home directory, you choose a subset of their folders to synchronize. This synchronization affects new, modified, and deleted files since the last synchronization.

  If users save files in locations that are not synchronized, the files remain local. If users delete files and then synchronize, those files are removed from both the local and network home folders. Also unlike some formal backup solutions, users cannot retrieve older versions of files, such as versions saved prior to the last synchronization.

- **You can't create mobile accounts when connected to a network through a virtual private network (VPN) connection.**

  You must create mobile accounts while directly connected to the network. After enabling a mobile account, you can then use VPN to connect to the network and synchronize your mobile account.

Strategies for Synchronizing Content

Administrators can enable and configure synchronization through Workgroup Manager. Users can configure synchronization through the Accounts preferences. The two methods of enabling mobile accounts have different synchronization capabilities. When you create mobile accounts through Workgroup Manager, you can choose to synchronize any folder within the user's home folder and choose whether to synchronize those folders at login or logout, or in the background. By contrast, when a user creates a mobile account through the Accounts preferences, he or she can only synchronize top-level folders like ~/Desktop or ~/Documents, and can only synchronize automatically (in the background) or manually.

A background synchronization occurs at the frequency you set, or whenever the user manually synchronizes. By default, when you enable background synchronization, synchronization occurs every twenty minutes. When the local home folder starts synchronizing with the network home folder, it checks the modification times for files located in both home folders. If the files have different modification times, then the newer file overwrites the older file.

Background synchronization should not be used with folders containing files that are accessed by multiple computers. This could cause users to load older, unsynchronized files. As an example, suppose a user saves a file on one computer and loads the same file on another computer. If that file was not synchronized to the server since its last save, the user loads an outdated version of the file located on the server. Alternatively, the file might not exist on the server because it was not synchronized yet. If the file was not synchronized from the server before loading it, the user either does not see the file or loads an outdated local version. Additionally, if a user using the same mobile account logs into two computers simultaneously, this might cause synchronization issues with the two computers, causing the computers to display error messages.

Login and logout synchronization should be carefully managed because a user's login and logout is delayed while files are synchronizing. If a user has a slow network connection or is synchronizing many files or large files, then the user must wait for synchronization to complete before using the system. If you want to synchronize parts of a user's ~/Library folder, you must use login and logout synchronization. Synchronizing the ~/Library folder retains users' bookmarks and individual application preferences,

Consider synchronizing smaller files like preference files at login and logout, while synchronizing larger files like movies in the background. Doing this reduces login and logout times (because only preference files synchronize) and movies synchronize throughout a user's session instead of while the user is trying to log out. You can further reduce network traffic by not synchronizing the movie folder and thus require users to only be able to access the movies folder locally. By balancing login and logout synchronization with background synchronization, you can reduce the time required for logging in and logging out while retaining consistent, synchronized home folders.

Setting Up Mobile Accounts for Use on Portable Computers

When distributing portable computers, you face a few special challenges not applicable to deploying stationary computers. For example, to ensure your portable computers remain managed while off of the network, you need to give users mobile accounts and prevent them from making local accounts or from changing settings to bypass management.

Configuring Portable Computers

When you distribute portable computers to users, you should configure those computers to prevent users from circumventing your management scheme.

To set up portable computers for use on your network.

1 Install the operating system, applications, and utilities.

Most computers come with Mac OS X installed. However, if you need to install a newer version, be sure the computer meets the minimum requirements for installing the operating system and any additional applications or utilities. If you want to take advantage of portable home directories, install Mac OS X version 10.4 or later.

2 Create local accounts on Mac OS X computers.

Create at least one local administrator account and create local user accounts as needed. Make sure the users' local account names are not easily confused with the users' network names. By creating an administrator account, this prevents the user from having administrator access, unless you specify it for the user. Administrator access gives the user the right to override many managed settings.

3 Set up computer lists on your server.

For Mac OS X computers, using Workgroup Manager to add portable computers to a computer list enforces preference management for all users of those computers. Additionally, if you create mobile accounts for a computer list rather than for specific users or groups, you can limit the creation of portable home directories to only specific computers. This way you can ensure that users who use several computers do not create portable home directories on each of those computers.

For more information about creating computer lists, see Chapter 6, "Setting Up Computer Lists." For instructions on creating mobile accounts, see "Creating a Mobile Account" on page 186.

Managing Mobile Clients Without Using Mobile Accounts

There are several situations in which you would not would not want to use mobile accounts for users of portable computers. This section details those scenarios and describes alternatives to using mobile accounts that allow you to manage portable computers.

Unknown Mac OS X Portable Computers

If a computer is not in a computer list, it is considered an unknown, or *guest* computer. If you can identify a computer using its Ethernet ID, you can add it to a computer list so that it will no longer be a guest computer.

You can use the Guest Computers computer list to manage guest computers on your network. This allows you to manage any portable computers with Mac OS X installed that join your directory domain. The preferences you manage in Workgroup Manager do not apply to Windows computers. If the users of guest computers log in using network or mobile accounts, their user and group managed preferences and account settings apply to them. For more information about how managed preferences interact when applied to users, groups, and computer lists, see "Understanding Managed Preference Interaction" on page 139.

For more information about setting up the Guest Computers account for Mac OS X users, see "Working with Guest Computers" on page 91.

Using Mac OS X Portable Computers with One Primary Local User

You can also distribute portable computers with only local accounts and not give users mobile or network accounts. This may reduce or eliminate the burden of maintaining dedicated directory domain servers and servers to store home folders. Even with local accounts, you can still manage users' computers when they use your network by adding their computers to a computer list.

When distributing portable computers, you can still retain some control over the computer when the user logs in with a local account while off the network. To restrict the user from full use of the computer, do not give him or her local administrator privileges. You can also set parental controls to further control the computer while off of the network. For more information about how to set parental controls, see Mac Help.

To restrict users from full access to the computer, create a local administrator account and a local user account on the computer. Give the user the login information for the local user account but not the local administrator account. With a non-administrator account, the user can't install software and can only save or delete files in his or her own home folder.

If you make the user the local administrator of the computer, you can deny the user the ability to turn off your management of the computer. However, in many cases, the local administrator can still override management settings.

If local users want to share files with other users over the network, they can use their ~/Public folder after enabling Personal File Sharing in the Sharing pane of System Preferences. Similarly, local users can connect to the computers of other users who have Personal File Sharing enabled.

If users also have network accounts, you might still prefer that they log in through their local accounts to reduce network traffic. They can connect to their network accounts through the "Connect to Server" command in the Finder's Go menu.

Using Max OS X Portable Computers with Multiple Local Accounts

Although mobile accounts often best suit portable computers, there are a few situations where using local accounts would provide advantages over using mobile accounts. An example is a school's wireless mobile lab, which might consist of twenty to thirty iBooks, an instructor's computer, an AirPort Extreme Base Station, and a printer, all located on a mobile cart. Since all of these computers are located on a mobile cart, a school could use this lab for multiple classrooms located throughout a campus.

When using a wireless mobile lab, it is very difficult to control who uses specific computers. Unlike distributing personal portable computers, where you know who uses which computer, or with stationary computers, where you can assign seating charts, it is hard to consistently use a distribution scheme for the wireless mobile lab. You could use stickers to label the computers to control distribution, but teachers would still have to monitor distribution to ensure students don't take the wrong computers. When a user creates a portable home directory on a computer, it uses some of the computer's hard disk space. If several dozen users create portable home folders on a computer, you could run out of hard disk space for the users' files.

Another consideration when using a wireless mobile lab is that the total network throughput is much more limited than a wired lab. If users have network accounts, any time they open or save files, it requires using the network, possibly slowing the network connections of other users. Although mobile accounts help alleviate these issues, frequent synchronization can also slow the network. Creating mobile accounts without any synchronized folders efficiently utilizes the network, but it can cause issues involving home folder proliferation. Additionally, users still have to copy and store their files in their network home folders.

To manage your cart's iBooks, you might 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 each class, such as an account for a History class, one for a Biology class, and so on. Each account has a local home folder but does not have administrator 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 folder for the generic account, you may want to periodically clean out that folder as part of your maintenance routine. Recommend to your students that they save their files to a network drop box to ensure their files are not deleted by your maintenance routine, and so that the students can access those files regardless of who uses the computer next.

Security Considerations for Mobile Clients

There are several security considerations for mobile clients that are not prevalent when deploying stationary clients. These considerations are relevant because of the mobile nature of the users' computers. When they are off your network, you can no longer monitor the actions of malicious users, nor can you control the network environment that your users join.

Preventing Unauthorized Computer Access

When you deploy client computers, there are several things you can do to better secure them. If you deploy mobile computers, you must take additional precautions because you cannot as easily control the actions of users on other networks.

Do the following to provide better local security for your computers:

- Require alphanumeric passwords with frequent expiration dates. You can set this and other strict password policy options as described in the Open Directory administration guide.
- Activate screen savers with minimum delay and require a password. For instructions on requiring a password for screensavers, search for "Locking your computer screen" in Mac Help.
- Set up open firmware passwords to disable computers from using single user mode, starting up the computer from other volumes, using NetBoot, and using target disk mode. For information about how to set up open firmware passwords, see the Apple Service & Support website article 106482 at:

  docs.info.apple.com/article.html?artnum=106482

Do the following to prevent unauthorized remote access to your computers:

- Disable SSH. Users logged in through SSH are not managed. They have the same privileges as local users in Terminal. To disable SSH, open Sharing preferences on the user's computer and deselect Remote Login.
- Disable other services that allow for external access, like FTP and Personal File Sharing. Enable services only when you require them. To disable FTP and Personal File Sharing, open the Sharing preferences on the user's computer and deselect Personal File Sharing and FTP Access. In this pane, you can also disable other services such as Windows Sharing and Personal Web Sharing.
- Use Apple Remote Desktop if you need secure remote access and management of computers. For more information about Apple Remote Desktop, see the Apple Remote Desktop administration guide.

Do the following to better secure your network resources:

- Create network views containing only the computers and servers your users need to access. For more information about network views, see Chapter 11, "Managing Network Views."
- Use access control lists (ACLs) to restrict access to your network's share points and shared folders. For more information about ACLs, see Appendix B, "ACL Permissions and Group Memberships Using GUIDs."
- Set up access control lists for servers to control which groups and users can access individual services hosted by a server. For more information about how to control access to services, see the getting started guide.

For additional security guidelines, see the Mac OS X Server security configuration guide at the National Security Agency (NSA) Security Configuration Guides website:

www.nsa.gov/snac/

Directory Services

The Directory Access application enables computers to access and use a directory server. There are three types of directory access policies: you can get directory services from a DHCP-supplied LDAP server, trusted binding, or untrusted binding. You should disable access to DHCP-supplied LDAP servers for computers, because they trust any directory domain they find when connecting to external networks. Untrusted binding is more secure than binding to a DHCP-supplied binding, but portable computers trust directory domains with the same DNS name or IP number as your directory server. Trusted binding is the most secure. It requires that both the portable computer and the LDAP directory server mutually authenticate.

For more information about how to choose and implement directory access policies, see the Open Directory administration guide.

FileVault for Mobile Clients

Mac OS X includes FileVault, which uses the latest government-approved Advanced Encryption Standard, providing 128-bit encryption. You can turn on FileVault for mobile accounts. After creating a mobile account, log in to the account. Once logged in, turn on FileVault in the Security pane of System Preferences. You need local administrator privileges and must set a master password, which allows you to unlock any local FileVault account.

Warning: If you do not use AFP to encrypt your files, synchronized files will transfer across your network in an unencrypted format. Copying files to network volumes will also send files across your network in an unencrypted format.

For more information about FileVault, search for "FileVault" in Mac Help.

Client Management Overview

9

This chapter provides an introduction to Mac OS X client management.

Client management is the centralized administration of your users' computer experience. It's usually implemented by:

- Managing access to network printers and to server-resident home folders, group folders, and other folders.
- Customizing the computer work environment of individual users, groups, and computers by defining preferences for user accounts, group accounts, and computer lists.

You can also take advantage of two additional client management options—installing and starting up client computers over the network (using NetBoot and Network Install) and day-to-day computer administration (using Apple Remote Desktop).

This chapter introduces each of these client management topics as they apply to users of Mac OS X computers.

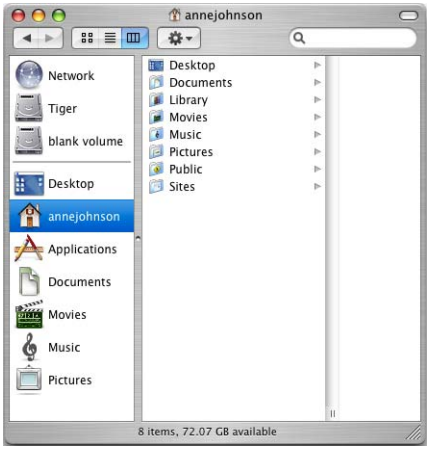
Using Network-Visible Resources

Mac OS X Server lets you make various resources visible throughout your network, so users can access them from different computers and various locations.

There are several key network-visible resources:

- **Network home folders.** A *home folder,* often referred to as a *home directory* or simply *home,* is a place for each Mac OS X user to keep personal files. A user with a record in a shared Open Directory directory domain may have a home folder that resides on the network, often on the same server where the user account resides.

  A home folder contains several folders—such as Desktop, Documents, and Public—to help organize information. After logging in, users access their network home folders by clicking the home icon in the Finder.



- **Group folders.** When you set up a group account for network users, you can associate a group folder with the group. A *group folder* is a place for group members to exchange information electronically. A group folder contains three folders by default—Documents, Library, and Public; the Public folder contains a Drop Box folder.

  Residing on the server for easy access throughout the network, a group folder can be shown in the Dock for access from wherever a user wants to work on group activities.

- **Other shared folders.** You can set up other folders on the server to provide users access to applications, handouts, announcements, schedules, and other files.

- **NetBoot and Network Install images.** You can use NetBoot images and Network Install images located on the server to simplify the setup of network users' computers.

  A user's computer can start up from a *NetBoot image* stored on the server. In fact, you can use the same computer for a science lab when it boots from one image and for a French lab when it boots from a different image. Each time a lab computer restarts, the system reflects the original condition of the selected boot image, regardless of what the previous student may have done on the computer.

  A *Network Install image* automatically installs preconfigured software on users' computers, making it easy to deploy the operating system, additional applications, and even custom computer settings remotely and without user interaction.

Customizing the User Experience

You manage a network user's work environment by defining preferences: settings that customize and control the user's computer experience. There are two panes in the Workgroup Manager Preferences pane, Overview and Details. The Overview tab manages predefined system preferences, while the Details tab can be used to manage preferences for any well behaved application or utility in Mac OS X.

The Overview tab is identical for Users and Groups:

An additional item, Energy Saver, appears for computer lists.

Many factors, including user responsibilities and security issues, determine what computer work environment a user should be presented with. In some cases, setting up informal usage guidelines may be sufficient. In other cases, extensively controlling the computer experience, with each system setting defined and locked and each application controlled, may be necessary. The preferences you define should implement system capabilities that best support your user and your business requirements.

The Power of Preferences

Many preferences, such as Dock and Finder preferences, are used to customize the appearance of the desktop. For example, you can set up Dock preferences and Finder preferences so that the work environment is dramatically simplified.

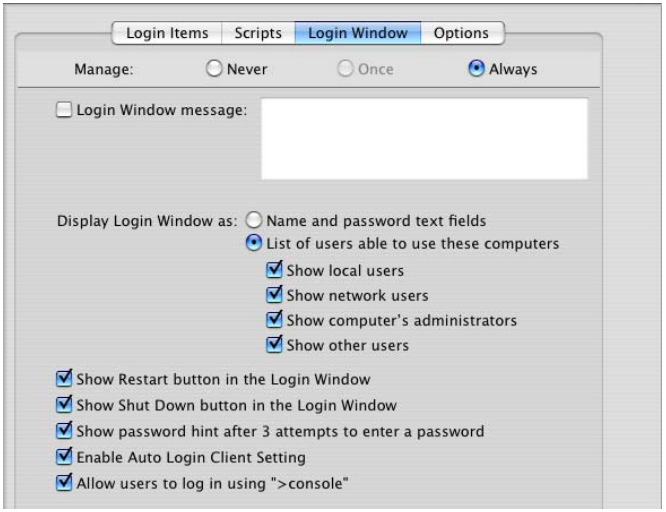
Other preferences are used to manage what a user can access and control. For example, you can set up Media Access preferences to prevent users from burning CDs and DVDs or making changes to a computer's internal disk.

Here's a summary of how preferences affect the appearance of the desktop and the activities a user can perform:

This preference	Tailors the work environment	Limits access and control	By letting you manage
Applications		x	The applications a user can open
Classic	x		Classic environment startup
Dock	x		The appearance and contents of the Dock
Energy Saver	x		Startup, shutdown, wake, sleep, and performance settings
Finder	x	x	The appearance of desktop icons and Finder elements
Internet	x		Default email and web settings
Login	x		The login experience
Media Access		x	Ability to use recordable media
Mobility	x		The creation of mobile accounts
Network	x	x	The proxy settings for accessing servers through a firewall
Printing		x	Which printers a user can use
Software Update	x		Which server to use for updates
System Preferences		x	Which system preferences are enabled on the user's computer
Universal Access	x		Hardware settings for users with special visual, auditory, or other needs

Designing the Login Experience

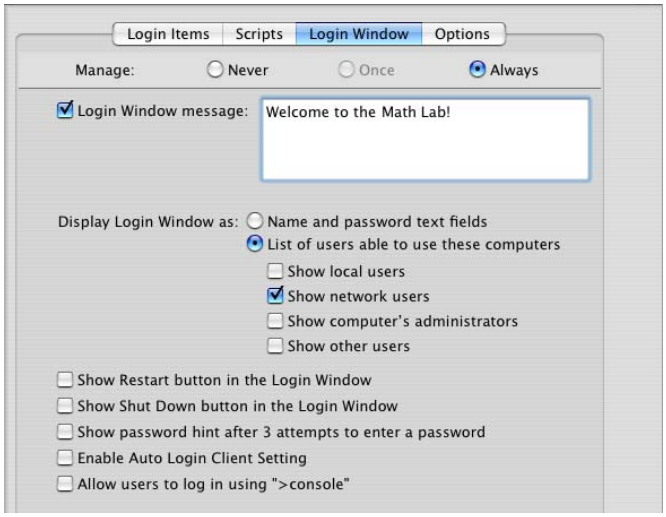
An example of the power of preference management is the ability to shape and control the user's login experience. You can set up Login preferences for computer lists to control the appearance of the login window. For example, if you set these options for the login window in Workgroup Manager:



and then the login window looks like this:

The first user in this case is the local computer administrator. The next three are users who have accounts that reside on the server, the last of whom has a mobile account.

If you want to set up a lab so that only users with network accounts can log in, set these options for the login window in Workgroup Manager:



and then the login window looks like this:

All four of these users have network accounts. Additionally, by disabling the Restart and Shut Down buttons, you prevent people who do not have network accounts from shutting down, restarting, or putting your computers to sleep. This login window also includes the message "Welcome to the Math Lab!," which serves as both a welcome and a warning to users that they are using math lab computers.

When a user selects his or her login name in the list, the user is prompted to type his or her password. If the user belongs to more than one workgroup, a list of available workgroups appears.

Network account users choose from workgroups in their directory domain, while local users get their workgroups from their local directory. It's possible for a user to belong to a group that doesn't appear in the list; it lists only workgroups that are allowed access by the computer list. Local administrators also have the option to not choose a workgroup and disable preference management.

Users can also select "Remember my choice," whereby for future logins, the workgroup picker is bypassed and the workgroup is automatically chosen for the users. Users can still change their workgroup by holding down the Option key as their password is being validated.

If the computer is associated with a computer list that supports local-only users, all workgroups given access to the computer by the computer list are listed after a local user logs in. The user can select any of them.

Any preferences that are associated with the user, the chosen workgroup, and the computer being used take effect automatically.

Improving Workflow

You can use preference management to improve workflow by limiting the total number of displayed applications and folders. You can also make these applications and folders more accessible by putting them in the Dock. You can also create multiple workgroups (groups with managed preferences), each of which has a Dock that is customized to show only the applications used by people in the group.

Applications can be stored locally on a computer's hard disk or on a server in a share point. If applications are stored locally, users can find them in the Applications folder. If applications are stored on a server, the user must connect to the server (by choosing Go > Connect to Server in the Finder) in order to locate and use the applications. Applications may also be made available through an automounted share point as the /Network/Applications mount record.

To make specific applications easy to find, you can use Dock Items preferences to place an alias for the My Applications folder in the user's Dock. The My Applications folder contains aliases to applications. Adding the My Applications folder might substantially delay the required login time for managed users, because Mac OS X has to search available disks to build the applications list every time the user logs in. For instructions on creating aliases to My Applications and other folders in a user's Dock, see "Adding Items to a User's Dock" on page 158.

You manage user access to local applications by creating lists of approved applications in the Applications preference. To set up a list of approved applications, see "Creating a List of Applications Users Can Open" on page 148. This list of approved applications determines what users find in the My Applications folder located in the Dock.

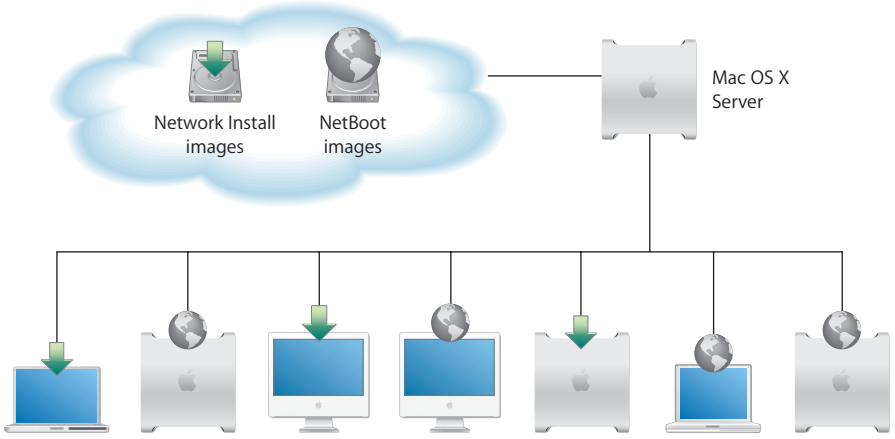
To prevent users from opening a Finder window to easily browse to other applications, use Simple Finder. For more information about using the Simple Finder, see "Setting Up Simple Finder" on page 165.

If you have set up a group folder, you can set up quick access to it when a user logs in to the workgroup with which the folder is associated. Users can use this group folder to facilitate file sharing between group members. For instructions on creating an alias to the group folder, see "Providing Easy Access to Group Folders" on page 157. To provide access to the group volume, which contains the /Public folder and a drop box for the group, see "Providing Easy Access to the Group Share Point" on page 177.

In addition to using managed preferences, you can also use network views to improve workflow. Network views control what users see when they click the Network icon in a Finder window. For more information about network views, see Chapter 11, "Managing Network Views," on page 207.

Using Images to Install Software and Start Up Computers

The key to fast initial setup of computers and rapid refresh of computers is the use of Network Install images, and NetBoot images that reside on the Mac OS X Server system. Computers start up using those images automatically.



Clients using Network Install or NetBoot images

You use Network Install images when you want to install software on computers or to refresh a computer once. You use NetBoot images when you want student computer environments to be refreshed every time the computer is started.

Using a network-based NetBoot image provides many advantages over starting up from a local hard drive:

- From the user's perspective, the NetBoot image is locked. It can't be accidentally or maliciously damaged. In a training lab where students may make mistakes or in a software development studio where system protection can't be used because of programming tool needs, you can use a NetBoot image to restore computers to their original state after each use. No matter what a student does while on the system, the image returns to the original condition at each startup.
- A network administrator who needs to perform maintenance doesn't need to carry a case full of diagnostic CDs. Instead, he or she can start up a system using a network image that contains all of the diagnostic and repair tools.
- Multiple images can be provided on the network from a single server, and multiple servers can provide a single image for optimum throughput.

  A server can host as many as 25 different images, so you can maintain a collection of customized software configurations for different workgroups and computers. For example, one image can be used for installing the latest applications needed by a particular team, and another image can be used for starting up computers in particular locations.

The system imaging and software update administration guide provides details about using System Image Utility to create images.

Day-to-Day Computer Administration

Administering networked computers also requires recordkeeping, help desk operations, and minor updates while users are logged in and working. To accomplish these and other day-to-day tasks, you use Apple Remote Desktop, which you can optionally purchase. It provides a remote management environment that simplifies student computer setup, monitoring, and maintenance:

- **Screen observation**. View student computer screens on your computer to monitor student activities or assess how well students are able to perform a particular task.
- **Screen control**. Show students how to perform tasks by controlling their screens from your computer.
- **Screen sharing**. Display your screen or a student's screen on student computers for training and demonstration purposes.
- **Screen locking**. Prevent students from using their computers when you want them to focus on other activities.
- **Text communications**. Exchange messages with one or more students, and host questions and requests from individual students.
- **Hardware and software management**. Audit hardware information and software that's installed. Search for specific files and folders on student systems.
- **Software distribution and startup**. Identify NetBoot or Network Install images for student computers to use. Initiate network installations and student computer shutdown and startup. Use Apple Remote Desktop to deploy application packages or new system updates instead of running Software Update on individual computers.
- **Troubleshooting**. Perform basic network troubleshooting by checking network traffic performance for all your workstations and servers.

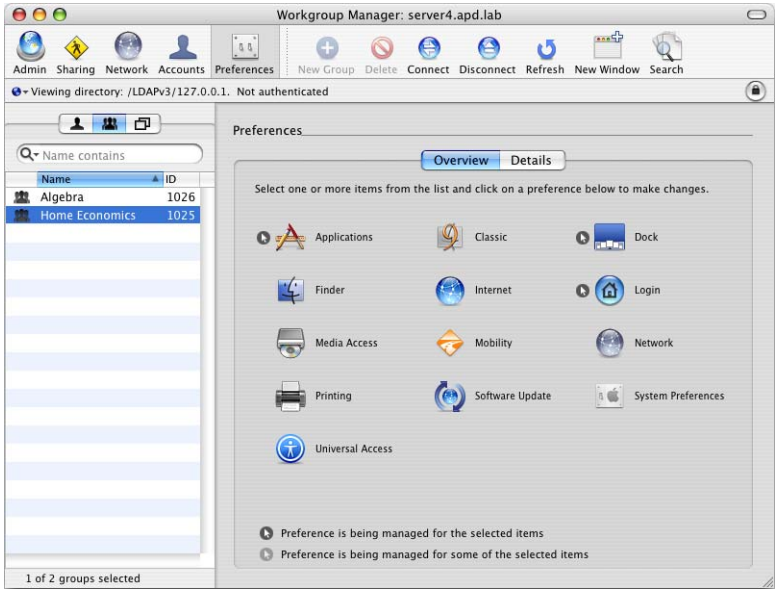
Managing Preferences

10

This chapter provides information about managing preferences for users, workgroups, and computers.

By managing preferences for users, workgroups, and computers, you can customize the user's experience and restrict users to accessing only the applications and network resources you choose.

You can use the Preferences pane in Workgroup Manager to manage preferences.



For an overview of using managed preferences to customize the user experience, see "The Power of Preferences" on page 130, and "Designing the Login Experience" on page 131.

How Workgroup Manager Works with Mac OS X Preferences

With Workgroup Manager you can set and lock certain system settings for users on their network. You can set preferences once and thereafter allow users to change them, or you can keep preferences under administrative control at all times (or you can leave preference settings unmanaged).

Workgroup Manager provides control over most major system and application preferences, in addition to various settings for users, groups, and computer lists. The preference editor controls the remainder of the applications that may require management.

Preference pane	What you can manage
Applications	Applications available to users. For more information, see "Managing Access to Applications" on page 148.
Classic	Classic startup settings, sleep settings, and the availability of Classic items such as Control Panels. For more information, see "Managing Classic Preferences" on page 151.
Dock	Dock location, behavior, and items. For more information, see "Managing Dock Preferences" on page 156.
Energy Saver	Performance options for Mac OS X client and server computers, Battery usage for portable computers, and sleep or wake options. For more information, see "Managing Energy Saver Preferences" on page 160.
Finder	Finder behavior, desktop appearance and items, and availability of Finder menu commands. For more information, see "Managing Finder Preferences" on page 164.
Internet	Email account preferences and web browser preferences. For more information, see "Managing Internet Preferences" on page 172.
Login	Login window appearance, mounted volumes, and items that open automatically when a user logs in. For more information, see "Managing Login Preferences" on page 174.
Media Access	Settings for CDs, DVDs, and recordable discs, plus settings for internal and external disks such as hard drives or floppy disks. For more information, see "Managing Media Access Preferences" on page 183.
Mobility	Creation of mobile account at login. For more information, see "Managing Mobility Preferences" on page 186.
Network	Configuration of specific proxy servers and settings for hosts and domains to bypass. For more information, see "Managing Network Preferences" on page 191.
Printing	Available printers and printer access. For more information, see "Managing Printing Preferences" on page 193.
Software Update	Specific server to use for software update service. For more information, see "Managing Software Update Preferences" on page 196.

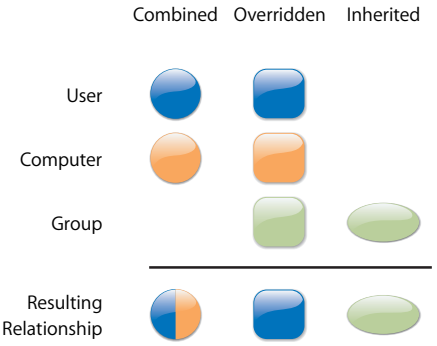
Preference pane	What you can manage
System Preferences	System preferences available to users. For more information, see "Managing Access to System Preferences" on page 197.
Universal Access	Settings to control mouse and keyboard behavior, enhance display settings, and adjust sound or speech for users with special needs. For more information, see "Managing Universal Access Preferences" on page 198.

Understanding Managed Preference Interaction

You can define preferences for user accounts, group accounts, and computer lists that are defined in a shared directory domain. A user whose account has preferences defined is referred to as a *managed user*. A computer assigned to a computer list with preferences defined is called a *managed computer*. A group with preferences defined is called a *workgroup*.

Energy Saver preferences and Login Window settings can be defined only for computer lists, but other preferences can be defined for users, workgroups, and computer lists.

The illustration below shows how managed preferences interact when the same preferences are set at multiple levels:



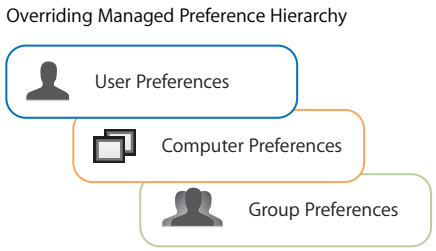
- Printing, Login, Applications, and some Dock preferences (involving items that appear in the Dock) are *combined*.

  For example, if you define printing preferences for users *and* computers, a user's printer list includes printers set up for both the user and the computer being used.

  Note: Managed System Preferences are combined, in that different settings defined in Workgroup Manager act collectively at login.

- Other preference settings defined at more than one level may be *overridden* at login.

The illustration below shows how overriding managed preferences interact when the same preferences are set at multiple levels:



When overriding preferences conflict, user preferences override both computer and group preferences, while computer preferences override group preferences.

For example, let's say you have different managed Dock preferences for users, workgroups, and computer lists. The Dock preferences for the user would take precedence, overriding and nullifying any Dock preferences set for workgroups or computers. If you do not manage any Dock preferences for the user, the computer list Dock preferences override and nullify any group Dock preferences.

An example of when overriding preferences is useful is in a school where you want to prevent all students from using recording devices attached to a school computer, except for students who serve as lab assistants. You could set up Media Access preferences for workgroups or computer lists to limit all students' access, but override these restrictions for lab assistants using Media Access settings at their user account level.

- *Inherited* preferences are preferences set at only one level.

  In some cases, you may find it easier and more useful to set certain preferences at only one level. 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 overriding or combining occurs, and the user inherits the preferences without competition.

Most of the time you'll use workgroup-level and computer-level preferences.

- Workgroup preferences are most useful if you want to customize the work environment (such as application visibility) for specific groups of users, or if you want to use group folders.

  For example, a student may belong to a group called "Class of 2011" for administrative purposes and to a workgroup called "Students" to limit application choices and provide a group shared folder for turning in homework. Another workgroup may be "Teacher Prep," used to provide faculty members access to folders and applications for their use only.

- Computer-level preferences are useful when you want to manage preferences for users regardless of their group associations. At the computer level, you might want to limit access to System Preferences, manage Energy Saver settings, list particular users in the login window, and prevent saving files and applications to recordable discs.

  Computer preferences also offer a way to manage preferences of users who don't have a network account but who can log in to a Mac OS X computer using a local account. (The local account, defined using the Accounts pane of System Preferences, resides on the user's computer.) You'd set up a computer list that supports local-only accounts. Preferences associated with the computer list and with any workgroup a user selects during login take effect. More about managing the login experience appears next.

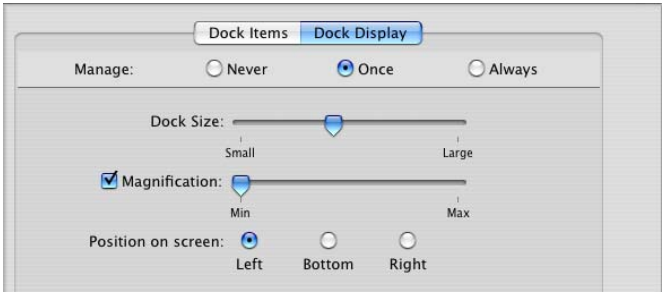
Setting the Permanence of Management

When you define preferences, you can choose to manage them Always or Once; they are set to Never by default.

- *Always* causes the preferences to remain in effect until you change them on the server. When properly designed, a Mac OS X application that conforms to standard preference conventions does not allow a user to modify preferences set to Always. You can use Always, for example, to make sure users can't add or remove Dock items.

  Some applications may allow the user to change the Always managed preference, but the next time the user logs back in, the preference will revert to the managed setting.

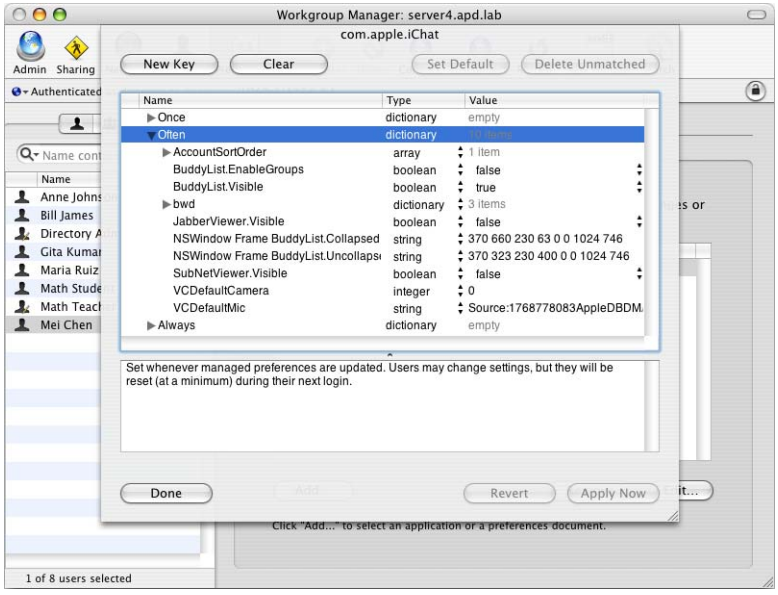
- *Once* is available for some preferences. You can create default preferences, which users can then modify and keep their modifications. These preferences are then effectively unmanaged. For example, you could set up a group of computers to display the Dock in a certain way the first time users log in. A user can change preferences you've set to Once, and the selected changes always apply to that user.



In the Overview Preference panes, you can set the following preferences to Once: Dock, Finder (Preferences and Views), Internet, Login (Login Items), Mobility (Login & Logout Sync and Background Sync panes of Rules), and Universal Access. For all other preferences, you must choose either Always or Never.

- *Never* lets a user control his or her own preferences. However, some preference settings, such as Accounts and Date & Time, require a local administrator's name and password before changes can be made. Never also means that the preferences are not managed at this account level, but may be managed at a different account level. For example, even if you set the Dock preference to Never for a particular user, the Dock preference could still be managed at the group or computer level.

Note: When using the preference editor (the Details view within the Preferences pane), you can set preferences to *Often*. Often settings are similar to Once settings, but are reapplied at every login. This management setting is useful for training environments. Users can customize their preferences to suit their needs during a session without any risk of affecting a future user's work experience. Additionally, some applications will only respond to preference management if set to Often.



Caching Preferences

Preferences can be cached on Mac OS X computers, so they remain in effect even when the computer is off the network:

- Computer preferences and preferences for any workgroups that can use the computer are cached.
- User preferences are always cached for users who have mobile accounts.

When a client computer is off the network, only users with local accounts or network users with mobile accounts on that computer can log in.

Managing Preferences

In Workgroup Manager, information about users, groups, and computer lists is integrated with directory services. After you set up the accounts, you can manage preferences for them. 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. Information about settings and preferences in user, group, or computer records is stored in a directory domain accessible to Workgroup Manager, such as the LDAP directory of an Open Directory master.

All preferences are stored in a record, which is either a user, group, or computer record. At login time, the managed client picks those out and puts them in a location where the final combined management list is applied to the user experience.

After user accounts, group accounts, and computer lists 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 should make sure each user you want to manage has either a network home folder or a local home folder on the server. For information about how to set up set up home folders for users, see Chapter 7, "Setting Up Home Folders."

Note: When you manage preferences for a user, group, or computer, an arrow icon appears next to the managed preference in the Preferences pane to indicate that you're managing that preference. You can select multiple users, groups, or computers to review managed preferences. If the arrow icon is dimmed, it means managed preference settings are mixed for the selected items.

About the Preferences Cache

The preference cache stores preferences for the computer list to which that computer belongs, preferences for groups associated with that computer, and preferences for users who have recently logged in on that computer. While this is true for network users, the cache is also used by workgroups for mobile accounts. The stored preferences can influence how a user is managed offline, and using the preference cache may improve performance.

The cached preferences can help you manage local user accounts on portable computers even when they're not connected to a network. For example, you can create a list of computers you want to manage, and then manage preferences for the computer list. Next, you can make these computers available to groups and then manage preferences for the groups. Finally, you can set up local user accounts on the computers. 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.

When you make a change that affects cached information for an account, Workgroup Manager sets a flag in the user account to indicate that change. When a user logs in, the client updates automatically.

Note: When you modify an account or preference setting, the preferences cache is updated automatically. New preferences take effect at the user's next login. If the user is already logged in while away from the network, the user must log out and log in again to update the preference cache.

Updating the Managed Preferences Cache at Intervals

You can update a computer's managed preference cache regularly. The computer checks the server for updated preferences according to the schedule you set. The cache is also updated automatically every time a change is made to any of the managed preferences within Workgroup Manager. If you change user account settings through the Inspector, you can still use Workgroup Manager to automatically update the cache at fixed intervals.

To set an update interval for the managed preferences cache:

1. In Workgroup Manager, click Accounts.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch to another directory, choose it from the globe pop-up menu.
3. Click the Computer Lists button and select one or more computer lists.
4. Click Cache.
5. Type in a number representing how frequently you want to update the cache, and 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.
6. Click Save.

   Note: Setting the cache interval to "0" turns off caching. Be aware that without caching, managed preferences do not take effect when the computer is disconnected from the network.

Updating the Preference Cache Manually

When you need to, you can manually update the managed preferences cache for every computer in a selected computer list.

To update the managed preferences cache:

1. In Workgroup Manager, click Accounts.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more computer lists.

4 Click Cache, and then click "Update Cache."

5 Click Save.

You can also update the cache on the client computer directly. Hold down the Option key when you log in on the client computer (using a local administrator name and password), and then click Refresh Preferences in the dialog displayed.

Warning: If you manually update the cache on the client computer while it is disconnected from the network, its preferences cache is deleted and the computer becomes unmanaged. The computer will become managed again when reconnected to the network and a user logs in to the directory domain.

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 or Once.

To manage user preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Click the Users button and select one or more user accounts from the list.

4 Click the icon for the preference you want to manage.

5 In each preference pane, select a Manage option.

In some cases (Printing and Media Access, for example), the management setting applies to all preferences rather than to individual panes within the preference.

6 Select preference settings or fill in information you want to use.

Some management settings are not available for some preferences, and some preferences are not available to some types of accounts.

7 When you've 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 time, 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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Groups button and select one or more group accounts from the list.
4. Click the icon for the preference you want to manage.
5. In each preference pane, select a Manage option.

   In some cases (Printing and Media Access, for example), the management setting applies to all preferences rather than to individual panes within the preference.
6. Select preference settings or fill in information you want to use.

   Some management settings are not available for some preferences, and some preferences are not available to some types of accounts.
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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more computer lists.

   If you are setting preferences for the Guest computers account, you must enable defining guest computer preferences. For instructions, see "Working with Guest Computers" on page 91.
4. Click the icon for the preference you want to manage.
5. In each preference pane, select a Manage option.

   In some cases (Printing and Media Access, for example), the management setting applies to all preferences rather than to individual panes within the preference.
6. Select preference settings or fill in information you want to use.

Some management settings are not available for some preferences, and some preferences are not available to some types of accounts.

7 Click Apply Now.

Editing Preferences for Multiple Records

You can edit preferences for more than one user account, group account, or computer list 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 has 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 then 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.

You can use the Once setting to create "default" settings. These are settings that, when saved, take effect the next time users log in. Users can then modify their settings and save their modified settings for future use. The Often setting does not allow users to save their preferences for future use, but they can modify their preferences for their current sessions.

To selectively disable preference management:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click the icon for a preference that is currently being managed.

5 In the pane whose preferences you no longer want to manage, select Never.

6 Click Apply Now.

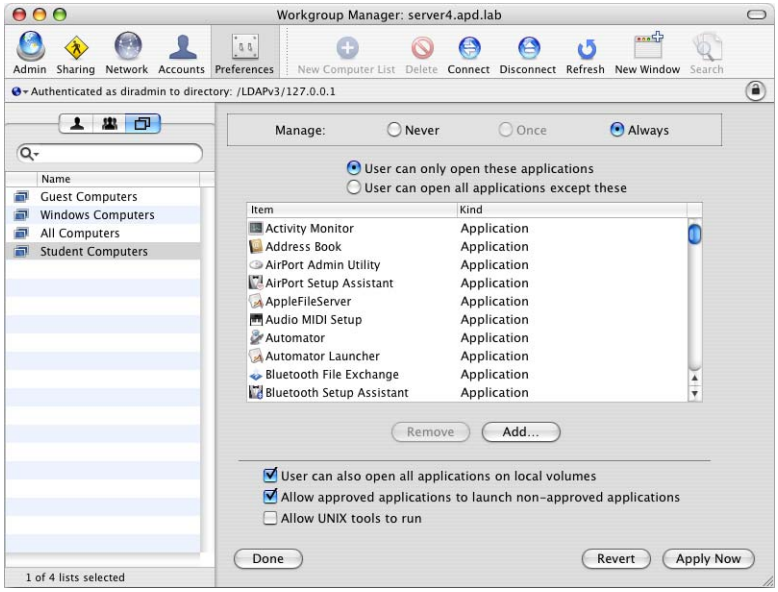
If preferences are managed at a higher level in the user, computers, groups hierarchy, setting the management value to Never may not result in unmanaged preferences.

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 management for an individual preference (for example, Dock), make sure the management setting is set to Never in each pane of that preference.

Managing Access to Applications

Use settings in the Applications pane to provide users with access to applications. You can create lists of "approved" applications that users are allowed to open, and you can allow users to open items on local volumes. You can also prevent applications from opening restricted applications.

Note: Applications are identified by their bundle ID. Since a clever user may change an application's bundle ID and thus defeat their access restrictions, the application restrictions should not be considered a barrier that no user can overcome.



Creating a List of Applications Users Can Open

There are two ways to control user access to applications. You can either provide access to a set of "approved" applications users can open, or you can prevent them from opening a set of "nonapproved" applications.

If you create a list of approved applications, users can open only the listed applications. (You can, however, allow applications to open "helper applications" that are not listed.) If you create a list of nonapproved applications, users can open any application that is not in that list.

To set up a list of accessible applications:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Applications.
5. Set the management setting to Always.
6. Select either "User can only open these applications" or "User can open all applications except these."
7. Add and remove items in the list.

   To browse for an application, click Add.

   To select multiple items, hold down the Command key.
8. When you have finished creating the list of applications, 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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Applications.
5. Set the management setting to Always.
6. Deselect "User can also open all applications on local volumes."
7. Click Apply Now.

Managing Access to Helper Applications

Sometimes, applications 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 to display the webpage.

When you make a set of applications available for users, groups, or computer lists, 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. Because an application can designate any other application as a helper application, for additional security, disallow helper applications.

When you set up a list of approved applications, you can choose whether to allow them to use helper applications that aren't in the approved-items list.

To manage access to helper applications:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Applications.
5. Set the management setting to Always.
6. Select "User can only open these applications."
7. If you haven't already created a list of approved applications, including helper applications, do so now.

   To browse for an application, click Add.
8. To allow access to helper applications, select "Allow approved applications to launch nonapproved applications."
9. Click Apply Now.

Controlling the Operation of UNIX Tools

Some applications, or the operating system, may occasionally require the use of non-application tools, such as the QuickTime Image Converter. These tools cannot be accessed directly, and generally operate in the background without the user's knowledge. You can, however, activate them using a command-line interface such as Terminal.

If you choose not to allow access to these types of tools, some applications may not function properly. Allowing this option enhances application compatibility and efficient operation, but for more strict security, you may choose not to do so.

To allow access to UNIX tools:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Applications.

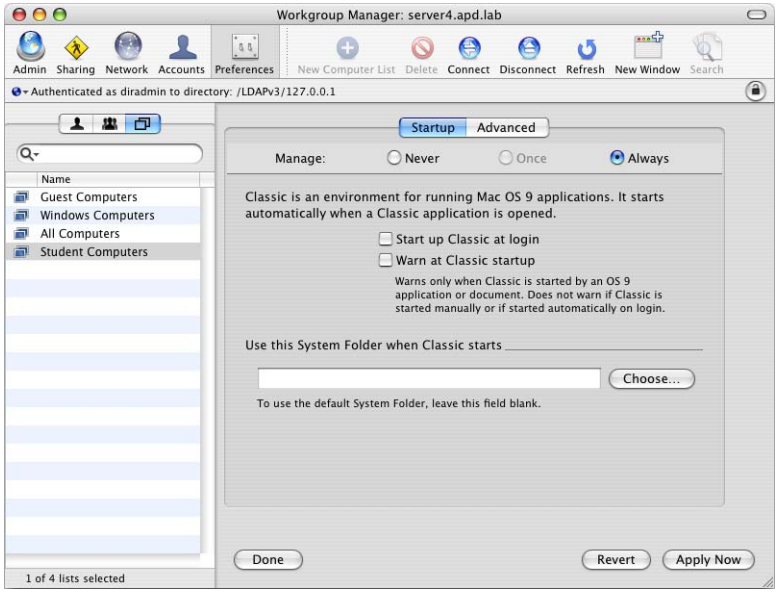
5 Set the management setting to Always.

6 Select "Allow UNIX tools to run."

7 Click Apply Now.

Managing Classic Preferences

Classic Preferences are used to set Classic startup options, select the Classic System Folder, set sleep options for the Classic environment, and make certain Apple menu items available to users. The Classic System Folder is a Mac OS 9 System Folder that contains the Mac OS 9 operating system. When users run Classic applications, they run Mac OS 9 from the Classic System Folder.



The table below describes what the settings in each Classic pane can do.

Classic preference pane	What you can control
Startup	Which folder is the Classic System Folder and what actions occur when Classic starts
Advanced	Items in the Apple menu, Classic sleep settings, and the user's ability to turn off extensions or rebuild the Classic desktop file during startup

Selecting Classic Startup Options

Workgroup Manager provides a number of ways to control how and when the Classic environment starts. If users often need to work with applications that run in Classic, it is convenient to have Classic start up immediately when a user logs in. If users rarely need to use Classic, you can have Classic start only when a user opens a Classic application or a document that requires such an application. You can also choose to display an alert when Classic starts, and give users the option of canceling Classic startup.

To work with various startup options for Classic:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Classic.
5. Click Startup.
6. Set the management setting to Always.
7. Select "Start up Classic on login to this computer" to start Classic immediately when a user logs in. When Classic starts up at login, the startup window is hidden and the user cannot cancel Classic startup.

   If users rarely need to use Classic, you can deselect this option and Classic starts up automatically when a user opens a document or an application that requires it. In this case, the Classic startup window is visible to users and they may cancel Classic startup.
8. Select "Warn at Classic startup" to show an alert dialog when Classic starts only after a user attempts to open a Classic application or document.

   Users can allow Classic startup to continue, or they can choose to cancel the process. If you don't want to allow users to interrupt Classic startup, deselect this option.
9. Click Apply Now.

Choosing a Classic System Folder

In most cases, there is only one Mac OS 9 System Folder on a given computer, and that folder is located on the Mac OS X startup disk. In this case, you don't have to specify a Classic System Folder. If a computer has multiple Mac OS 9 System Folders on the startup disk and you haven't set a specific path to one folder, users see an error message and are unable to use Classic.

If there is more than one Mac OS 9 System Folder on a computer's startup disk or if you want to use a Mac OS 9 System Folder located on a different disk, you should enforce the use of a specific folder when Classic is in use. It is important that if you specify a path to the folder's location, all clients should have the Mac OS 9 System Folder in the same relative location on their hard disks.

If multiple Mac OS 9 System Folders are available and you don't enforce any settings in the Startup pane of the Classic preference, users may choose from among available Mac OS 9 System Folders if they have access to the Classic pane of System Preferences.

To choose a specific Classic System Folder:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Classic.
5. Click Startup.
6. Set the management setting to Always.
7. Enter in the path to the Classic System Folder you want to use; for example:

   /Volumes/*VolumeName*/System Folder/

   Or click Choose to browse for the folder you want.

   Be sure the path to the Classic System Folder on the client computer is the same as the path to the Classic System Folder on the administrator computer.
8. Click Apply Now.

Allowing Special Actions During Restart

If managed users have access to the Classic pane of System Preferences, they can click the Start/Restart button in the Classic pane to start or restart Classic. You can allow users to perform special actions, such as turning off extensions, starting or restarting Classic, or rebuilding the Classic desktop file, from the Advanced pane of Classic system preferences. You may want to allow this only for specific users, such as members of your technical staff.

To allow special actions during restart:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.

4 Click Classic.

5 Click Advanced.

6 Set the management setting to Always.

7 Select "Allow special startup modes."

8 Select "Allow user to rebuild desktop" if you want to allow users to rebuild the Classic desktop file. Deselecting this option disables the Rebuild Desktop button in the Advanced pane of Classic system preferences.

9 Click Apply Now.

Controlling Access to Classic Apple Menu Items

Classic managed preference options allow you to control access to certain items in Classic's Apple menu, including Mac OS 9 control panels, the Chooser and Network Browser, and other Apple menu items. You can choose to show or hide all, some, or none of these items in the Apple menu.

If an item is hidden, users cannot access that item from the Apple menu; however, there may be alternative methods of access, such as starting the Chooser by navigating to it within the Mac OS 9 System Folder. If you want to further limit user access to these items, you can use the Applications preferences in Workgroup Manager to determine which specific applications a user may or may not open. For more information, see "Managing Access to Applications" on page 148.

Note: Disallowing access to the Chooser may affect what happens when a client attempts to print from Classic if printer management is also enforced. If users cannot access the Chooser, they cannot set up new printers or switch between types of printers (such as PostScript and non-PostScript printers).

To hide or show items in the Apple menu:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Classic.

5 Click Advanced, and set the management setting to Always.

6 Select "Hide Control Panels" to remove this item from the Apple menu. Deselect this option to show this item.

7 Select "Hide Chooser and Network Browser" to remove both of these items from the Apple menu. Deselect this option to show these two items.

8 Select "Hide other Apple menu items" to hide remaining Apple menu items. This group includes items such as Calculator, Key Caps, and Recent Applications. Deselect this option to show these Apple menu items.

9 Click Apply Now.

Adjusting Classic Sleep Settings

When no Classic applications are open, Classic goes 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.

In some circumstances, you may need to use applications that operate in the background without the user's interaction or knowledge. If a background application is in use when Classic enters sleep mode, that application suspends its activity. If you want to keep the application running, you can set Classic's sleep setting to Never.

To adjust Classic sleep settings:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Classic.

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.

Maintaining Consistent User Preferences for Classic

Ordinarily, Classic looks for an individual user's data for Mac OS 9 preferences in the Mac OS 9 System Folder. If a user uses more than one computer or if multiple users work on the same computer, you should make sure Classic uses preferences from the Home folder in ~/Library/Classic/ so that preferences remain consistent for each user.

If you choose not to use preferences in the user's own Home folder, a user's Mac OS 9 data is stored in the Mac OS 9 System Folder and is not kept separate from other user's data. In this case, users share preferences and any changes made by the last user are in effect when the next user logs in.

To choose where Classic user preferences are stored:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Classic.

5 Click Advanced and set the management setting to Always.

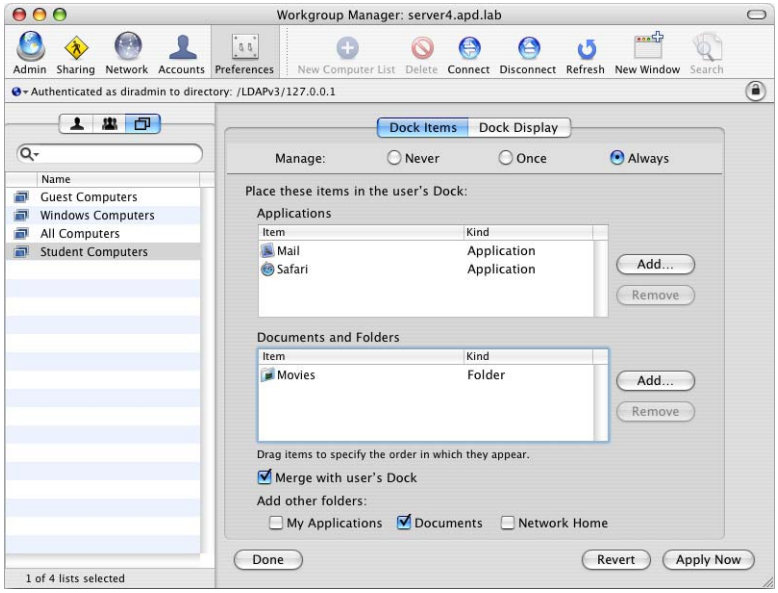
6 Select "Use preferences from home folder" to maintain consistent Classic preferences for each user.

Deselect this option to use the local Mac OS 9 System folder for all Classic user preferences.

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.



The table below describes what the settings in each Dock pane can do.

Dock preference pane	What you can control
Dock Items	Items and their position in a user's Dock
Dock Display	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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Dock.
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, and 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 appears 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.

Providing Easy Access to Group Folders

After you have set up a group volume, you can make it easy for users to locate the group directory by placing an alias in the user's Dock. The group directory contains the group's Library folder, Documents folder, and Public folder (including a drop box). If you need help setting up a group share point, see "Creating a Group Folder" on page 86.

If the group directory is not available when the user clicks the group folder icon, the user must enter a user name and password to connect to the server and open the directory.

Note: This preference setting applies only to groups. You cannot manage this setting for users or computers.

To add a Dock item for the group directory:

1. If you haven't set up a group share point, do so before you proceed.
2. In Workgroup Manager, click Preferences.
3. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
4. Click the Groups button and select one or more group accounts from the list.
5. Click Dock.
6. Click Dock Items.
7. Select a management setting (Once or Always).

   If you select Once, the group folder icon appears in the user's dock initially, but the user can remove it.
8. Select "Add group folder."
9. Click Apply Now.

If you change the location of the group share point, be sure to update the Dock item for the group in Workgroup Manager.

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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Dock.
5. Click Dock Items.
6. Select a management setting (Once or Always).

   If you select Once, the user can add and remove Dock items. The user cannot remove items from the Dock with Always selected.

7 To add individual applications, 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. Any user-added items are located after your listed applications.

8 Select My Applications, Documents, or Network Home to add one or more of these items to the user's Dock.

The My Applications folder contains aliases to all approved applications listed in the Applications preference pane. If you do not manage the Applications preference, all available applications are shown. If you enable Simple Finder, you should display the My Applications folder.

The Documents folder is the Documents folder found in the user's home folder.

The Network Home folder is the network home folder for users with network accounts. For users of mobile accounts, it is their network home folders, not their local home folders.

9 Deselect "Merge with user's Dock" to replace the user's current Dock with your selected items.

10 When you have finished adding Dock items, click Apply Now.

Preventing Users from Adding or Deleting Items in the Dock

Ordinarily, users can add items to their own Docks, but you can prevent this. Users can't remove items you add to the Dock while Always ("Manage these settings") is selected.

To prevent users from adding items to their Docks:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Dock.

5 Click Dock Items, and then set the management setting to Always.

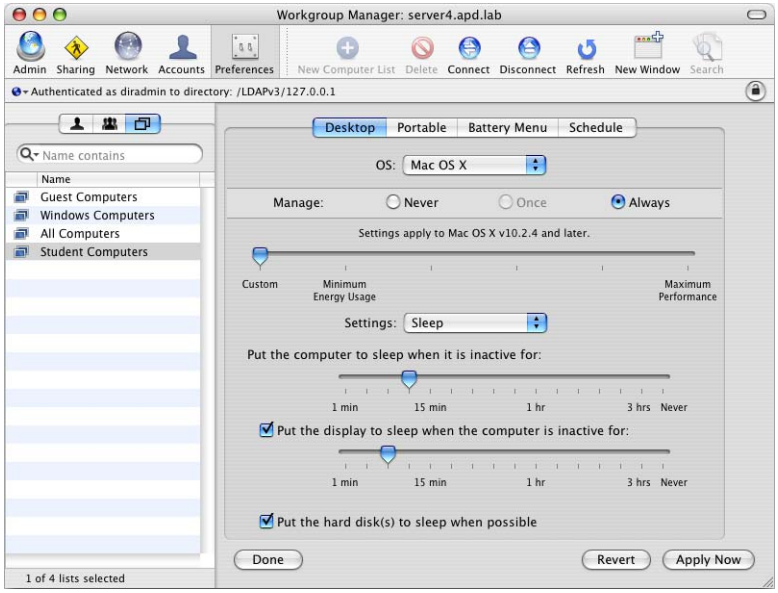
6 Deselect "Merge with user's Dock."

7 Click Apply Now.

Managing Energy Saver Preferences

Energy Saver preference settings help you save energy and battery power by managing wake, sleep, and restart timing for servers and client computers.

You can configure Energy Saver preferences for desktop and portable computers. Desktop computers and portable computers differ in that portable computers can run on battery power.



The table below summarizes what you can control with the settings in each Energy Saver pane.

Energy Saver preference pane	What you can control
Desktop	Sleep timing for the computer, display, and hard disk(s), and wake and restart options for Mac OS X and Mac OS X Server
Portable	Processor performance setting, sleep timing similar to Desktop, and wake and restart options for Adapter and Battery power sources
Battery Menu	Whether the battery status indicator appears for users
Schedule	Regular schedules for startup or shutdown

Using Sleep and Wake Settings for Desktop Computers

Putting a computer to sleep saves energy because it turns off the display and stops the hard disk from running. Waking up from sleep is faster than starting up your computer.

You can use Workgroup Manager's Energy Saver preference settings to put client computers to sleep automatically after a specified period of inactivity. Other settings enable you to wake or restart the computer when certain events happen.

To set sleep and wake settings:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Energy Saver.
5. Click Desktop.
6. Choose either Mac OS X or Mac OS X Server from the OS pop-up menu and set the management setting to Always.
7. To adjust sleep settings, choose Sleep from the Settings pop-up menu.

   Move the slider to set how long the desktop computer waits to enter sleep mode. The default setting is 1 hour. The computer does not enter sleep mode if the slider is set to Never.

   To use a different time interval for the computer's display, select "Put the display to sleep when the computer is inactive for" and move the slider. The interval cannot be longer than the computer's sleep setting.

   To put the hard disks to sleep during periods of inactivity, select "Put the hard disk(s) to sleep when possible."
8. To set wake and restart settings, choose Options from the Settings pop-up menu.

   To wake the computer when the modem is activated, select "Wake when the modem detects a ring."

   To wake the computer when an administrator attempts access remotely, select "Wake for Ethernet network administrator access."

   To make sure the computer restarts if the power fails, select "Restart automatically after a power failure." Deselect this option to disable automatic restart.
9. Click Apply Now.

To manually wake up a sleeping computer or display, the user can click the mouse or press a key on the keyboard.

Working with Energy Saver Settings for Portable Computers

You can use Energy Saver Portable settings to vary sleep and wake responses in addition to processor performance settings depending upon what power source a portable computer is using (either an adapter or a battery). You can also have the computer restart automatically if power fails suddenly.

Users should be encouraged to use the computer's adapter when possible to save battery power.

To manage portable computer settings:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Energy Saver.
5. Click Portable.
6. Choose either Adapter or Battery from the Power Source pop-up menu and set the management setting to Always.
7. To adjust sleep settings, choose Sleep from the Settings pop-up menu.

   Move the slider to set how long the portable computer waits to enter sleep mode. The default setting is 10 minutes. The computer does not enter sleep mode if the slider is set to Never.

   To use a different time interval for the computer's display, select "Put the display to sleep when the computer is inactive for" and move the slider. The interval cannot be longer than the computer's sleep setting.

   To put the computer to sleep during periods of inactivity, select "Put the hard disk(s) to sleep when possible."
8. To set wake, restart, and processor performance settings, choose Options from the Settings pop-up menu.

   To wake the computer when the modem is activated, select "Wake when the modem detects a ring".

   To wake the computer when an administrator attempts access remotely, select "Wake for Ethernet network administrator access."

   For client computers with Mac OS X version 10.3 or later, you can select "Allow power button to sleep the computer." If enabled, when users press the power button without holding down the power button for a prolonged period, they put the computer in sleep mode.

   To make sure the computer restarts if the power fails, select "Restart automatically after a power failure." Deselect this option to disable automatic restart.

   Select either Highest, Automatic, or Reduced in the Processor Performance pop-up menu. For computers using an adapter, the recommended setting is Highest. For computers using a battery, the recommended setting is Automatic.
9. Click Apply Now.

To manually wake up a sleeping computer or display, users can click the mouse or press a key on the keyboard.

Displaying Battery Status for Users

Portable computers use a battery either as a direct power source while disconnected from external power, or as a backup power source while connected to external power. When battery power is too low for the computer to function, the computer puts itself to sleep to conserve energy. When a user reconnects the computer to a functional power source (for example, by inserting a fresh battery or connecting a power adapter), the user can wake the computer and begin working again.

Users should be encouraged to monitor battery status when roaming free and use a power adapter when possible to maintain a fully charged battery.

To show battery status in the menu bar:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Energy Saver.
5. Click Battery Menu and set the management setting to Always.
6. Select "Show battery status in the menu bar" to display the battery menu. To disable the battery menu, deselect this option.
7. Click Apply Now.

Scheduling Automatic Startup, Shutdown, or Sleep

You can choose to have computers start up, shut down, or sleep at specific times on specific days of the week. Scheduling shutdown or sleep can help you conserve energy during predictable times of user inactivity, such as after work hours, on weekends, or after a class is finished. Scheduling startup automatically can allow you to conveniently prepare a lab or classroom for immediate use.

To schedule automatic actions:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Energy Saver.
5. Click Schedule.
6. Choose either Mac OS X or Mac OS X Server from the OS pop-up menu and set the management setting to Always.

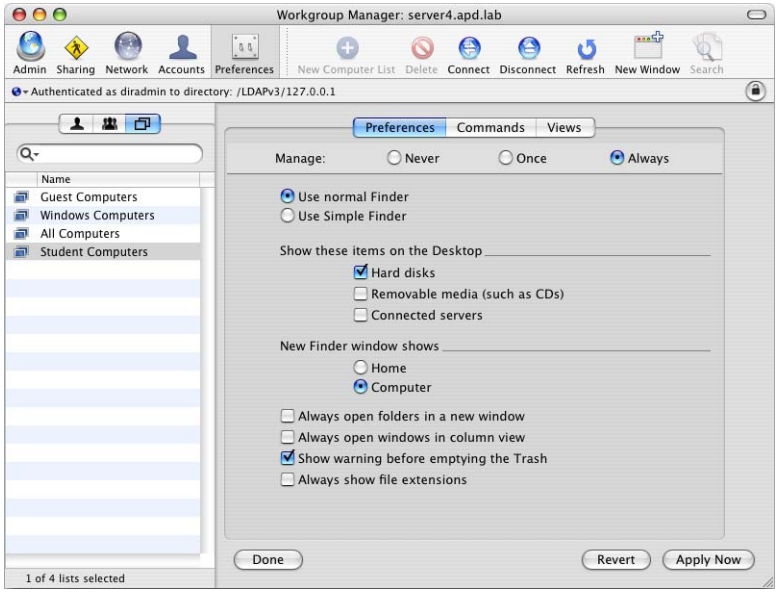
7 To schedule automatic startup, select "Start up the computer" and choose a day or range of days (Weekdays, Weekends, or Every Day) from the pop-up menu. Then, enter a time in the time field. To disable scheduled startup, deselect this option.

8 To schedule automatic sleep or shutdown, select the checkbox and then choose either Sleep or Shut Down from the pop-up menu. Next, choose a day or range of days (Weekdays, Weekends, or Every Day) from the pop-up menu. Then, enter a time in the time field. To disable scheduled sleep or shutdown, deselect this option.

9 Click Apply Now.

Managing Finder Preferences

You can control various aspects of Finder menus and windows. By controlling Finder menus and windows, you can improve or control workflow. For example, you can simplify the user experience by enabling Simple Finder. You can also prevent users from burning media or from ejecting disks.



The table below summarizes what you can do with each Finder preference pane.

Finder preference pane	What you can control
Preferences	Finder window behavior, Simple Finder, whether open items appear on the desktop, filename extension visibility, and the Empty Trash warning dialog.
Commands	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. Settings in the Commands pane let you control whether certain commands are available to users.
Views	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 folder of the computer.

Setting Up Simple Finder

You can select either the normal Finder or Simple Finder as the user environment. The normal Finder looks and acts like the standard Mac OS X desktop. Simple Finder removes the ability to use a Finder window to access applications or modify files. This limits users to accessing only what is in the Dock. If you enable Simple Finder, users cannot mount network volumes. With Simple Finder enabled, users cannot create folders or delete files.

In addition to using Workgroup Manager, you can set up Simple Finder on a client computer (locally) using System Preferences. When you use Workgroup Manager to apply the Simple Finder environment and the feature is not in use on the local computer, only the client's Finder is affected; Dock and Application access settings must be managed separately. You can set up the Simple Finder on the local computer, and use the application and Dock management features in Workgroup Manager to add Dock items and application access.

Important: For client computers using Mac OS X versions 10.2 through 10.2.8, don't turn on Simple Finder for users who log in to a workgroup with its own group folder. These users can't use applications because Simple Finder prevents access to the group folder.

To turn on Simple Finder:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Finder.
5. Click Preferences and select a management setting (Always).

6 If you select Always, you can select either "Use normal Finder" or "Use Simple Finder."

If you select Once, the account can only use the normal Finder.

7 Click Apply Now.

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 folder when a user clicks the Computer icon in a Finder window toolbar.

To hide disk and server icons on the desktop:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Preferences 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 which folder 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 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Preferences and select a management setting (Once or Always).

6 Under "New Finder window shows," specify the items you want to display.

Select Home to show items in the user's home folder.

Select Computer to show the top-level folder, which includes local disks and mounted volumes.

7 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.

8 Select "Always open windows in Column View" to maintain a consistent view among windows.

9 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 don't want users to see this message, you can turn it off.

To hide the Trash warning message:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Preferences and select a management setting (Once or Always).

6 Deselect "Show warning before emptying the Trash."

7 Click Apply Now.

Making Filename Extensions Visible

A filename extension usually appears at the end of a file's name (for example, ".txt" or ".jpg"). Applications use the filename extension to identify the file type.

To make filename extensions visible:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Select a management setting (Once or Always).

6 Select "Always show file extensions."

7 Click Apply Now.

Controlling User Access to Remote Servers

Users can connect to a remote server by choosing 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 use this menu item, you can hide the command.

To hide the "Connect to Server" command:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Finder.
5. Click Commands and set the management setting to Always.
6. Deselect "Connect to Server."
7. Click Apply Now.

Controlling User Access to an iDisk

If users want to connect to an iDisk, they can choose 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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Finder.
5. Click Commands and set the management setting to Always.
6. Deselect "Go to iDisk."
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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

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 ability, you can hide the Burn Disc command in the Finder's File menu.

To hide the Burn Disc command:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

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 works only with CD-R, CD-RW, or DVD-R discs. Only a SuperDrive can burn DVD-Rs.

Controlling User Access to Folders

Users can open a specific folder by choosing 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 ability, you can hide the command.

To hide the "Go to Folder" command:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Commands and set the management setting to Always.

6 Deselect "Go to Folder."

7 Click Apply Now.

Removing Restart and Shut Down from the Apple Menu

If you don't want to allow users to restart or shut down the computer they're using, you can remove the Restart and Shut Down commands from the Apple menu.

To hide the Restart and Shut Down commands:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Commands and set the management setting to Always.

6 Deselect Restart and Shut Down.

7 Click Apply Now.

As an additional preventive measure, you can make the Restart and Shut Down buttons unavailable (dimmed) from the login window, by using settings in Login preferences. For instructions, see "Managing Login Preferences" on page 174.

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're arranged.

To set preferences for the desktop view:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Views, and then select a management setting (Once or Always). This setting applies to options in all three views.

6 Click Desktop View.

7 Drag the slider to adjust the icon size.

8 To keep items aligned in rows and column, select "Snap to grid."

To arrange items by criteria such as name or type (for example, all folders grouped together), select "Keep arranged by," then choose a method from the pop-up menu.

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 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 folder, showing hard disks and disk partitions, external hard disks, mounted volumes, and removable media (such as CDs or DVDs).

To set preferences for the default and computer views:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Views, and then select a management setting (Once or Always). This setting applies to options in all three views.

6 Click Default View.

7 Drag the Icon View slider to adjust the icon size.

8 Select how you want to arrange icons.

Select None to allow users to place items anywhere on the desktop.

Select "Snap to grid" to keep items aligned in rows and columns.

Select "Keep arranged by," and 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 "3/24/05," 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.

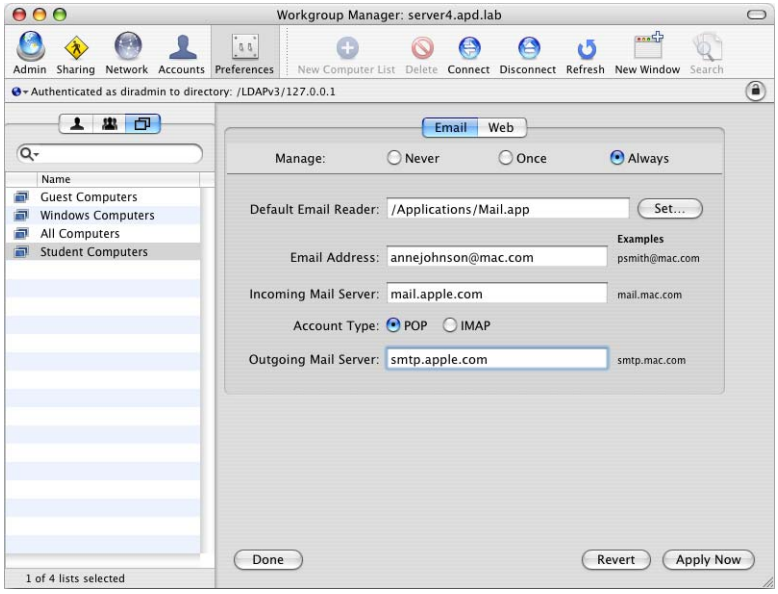
Select a size for icons in a list.

10 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.

11 Click Apply Now.

Managing Internet Preferences

Internet preferences let you set email and web browser options. Some Internet browser or email applications may not support these settings.



The table below describes what the settings in each Internet pane can do.

Internet preference pane	What you can control
Email	Preferred email application and email information
Web	Preferred web browser and URLs for the home page and search page

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.

Note: Some mail applications may ignore these settings.

To set email preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Internet.
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 default URL for your browser using the Home Page location. Use the Search Page location to specify a search engine URL.

Note: Some web browsers may ignore these settings.

To set web preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

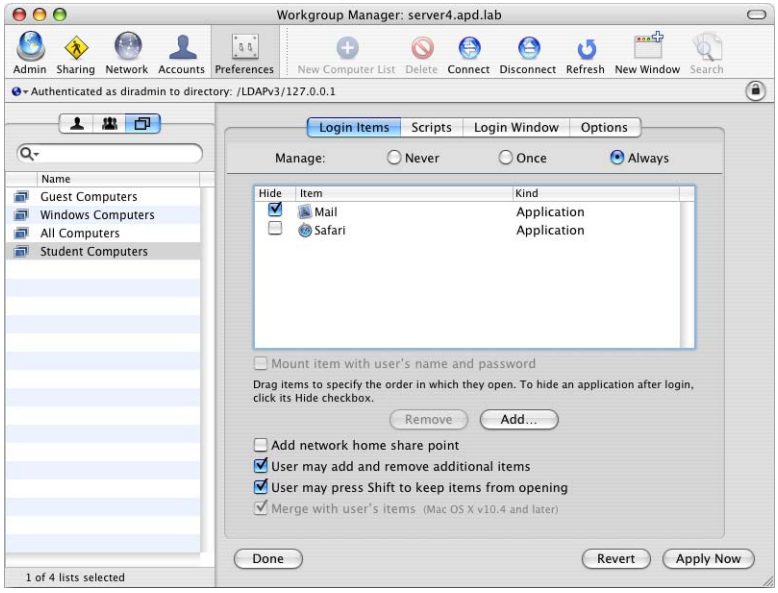
   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Internet.
5. Click Web and select a management setting (Once or Always).
6. To set 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 options for user login, provide password hints, and control the user's ability to restart and shut down the computer from the login window. You can also mount a group volume or make applications open automatically when a user logs in.



The table below summarizes what you can do with the settings in each Login pane.

Login preference pane	What you can control
Login Items	Access to the group volume; which applications open automatically for the user; enable users to manage opening items
Scripts	*For computer lists only:* Specify a script to run during login or logout; execute or disable the client computer's own LoginHook or LogoutHook scripts
Login Window	*For computer lists only:* The appearance and function of items in the Login window; which users are listed if "List of users" is specified
Options	*For computer lists only:* Allow Fast User Switching; how many minutes of inactivity result in the user being logged out

Scripts, Login Window, and Options can be managed for computers only, not for users or groups.

Specifying How a User Logs In

Depending on the settings you choose, a user sees either a name and password text field or a list of users in the login window. These settings apply only to computer lists.

To set up how a user logs in:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more computer lists.
4. Click Login.
5. Click Login Window and set the management setting to Always.
6. To require the user to type his or her user name and password, select "Name and password text fields."
7. To allow a user to select his or her name from a list, select "List of users able to use these computers."

   If you decide to use a list of users, select categories of users you want to display in the list. To ensure that a type of user doesn't show up in the list, deselect the corresponding setting. If you allow unlisted users to log in, you can select "Show other users."

   In addition to controlling computer access through these login window display settings, you can control access to computers per computer list by selecting a group in the Access pane for computer lists in Workgroup Manager. The preferences you set in this pane might conflict with the login window display managed preferences. For more information about how to use the Access pane, see "Restricting Access to Computers" on page 97, "Making Computers Available to All Users" on page 98, and "Using Local User Accounts" on page 98.
8. You may want to prevent users from logging in using the Darwin console (command-line interface) to evade management. To disable Darwin login, deselect "Allow users to log in using >console."
9. To disable automatic login as a specific user when the computer starts up, deselect "Enable Auto Login Client Setting."

   In case you decide to use this setting, you must set up automatic login on the client computer. Open System Preferences, click Accounts, click Login Window, select "Enable Auto Login Client Setting," choose a user from the pop-up menu, and provide the correct password for that user account.
10. When you have finished selecting managed login settings, click Apply Now.

Opening Items Automatically After a User Logs In

You can open frequently used items for a user. You can also hide items that open automatically to help prevent screen clutter, while still making the item easily accessible.

Items open in the order they appear in Login Items preferences (you can specify the order). As items open, they "stack" on top of one another; the last item is closest to the top. For example, if you specify three items to open (and none is 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.

A user can stop login items from opening by holding down the Shift key during login until the Finder appears on the desktop; you can turn off this feature.

To make an item open automatically:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Login.
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 items" if you don't want users to have this ability. This checkbox is available only if Login Items preferences are always managed. If you manage Login Items preferences once, a user can remove any items added to the login list.

   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 items from opening." (This checkbox is available only if Login Items preferences are always managed.)
10. If you select Once, you can click "Merge with user's items." This can have two results, depending on whether the user already has items in their login list.

If the user already has items listed in their login list, either through the user adding them or from having items previously added through preference management, merging opens only login items that appear both on the user's list and your list. If the user's login list does not include any items, all managed login items appear. If you do not select "Merge with user's items," all login items on either list open.

11 Click Apply Now.

Providing Access to a User's Network Home Folder

This setting is used primarily for mobile accounts on computers running Mac OS X version 10.3 to Mac OS X version 10.3.9. When any user logs in while connected to the network, the share point with the user's original home folder (located on the server) is mounted on the desktop.

You should not provide access to a user's network home folder to users with mobile accounts on Mac OS X version 10.4 or later. Mac OS X version 10.4 introduces portable home directories, which provide a synchronized subset of the user's local and network home folders. If a user modifies files in both the local and network home folders, when the two home folders synchronize, the newer modifications take precedence, which could surprise and confuse the user. Additionally, users could be confused by having multiple folders titled with their user names and similarly named folders like Documents, Music, and others.

To automatically mount the Network Home:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select a mobile user account in the account list.

4 Click Login.

5 Click Login Items.

6 Select a management setting (Once or Always).

7 Select "Add network home share point."

8 Click Apply Now.

Providing Easy Access to the Group Share Point

After you have set up a group share point, you can make it easy for users to locate group folders by accessing the share point automatically at login. (For information about setting up a group share point, see "Creating a Group Folder" on page 86.)

Note: This preference setting applies only to groups. You cannot manage this setting for users or computers.

To add a login item for the group share point:

1. If you haven't set up a group share point and group folder, do so before you proceed.
2. In Workgroup Manager, click Preferences.
3. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
4. Click the Groups button and select one or more group accounts from the list
5. Click Login.
6. Click Login Items.
7. Set the management setting to Always.
8. Select "Add group share point."
9. Select the newly added group share point item.

   If you don't want the group share point to appear in the Dock, select the Hide checkbox.
10. Make sure "Mount with user's name and password" is selected.
11. Click Apply Now.

When the user logs in, the computer connects to the group share point with the user name and password given at login. If you manage Finder preferences and choose not to show connected servers, the group volume's icon does not appear on the desktop. However, the user can find the volume by clicking Computer in a Finder window.

If you change the location of the group share point, be sure to update the login item for the group in Workgroup Manager.

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 can make these buttons unavailable.

You may also want to remove the Restart and Shut Down commands from the Finder menu. (For instructions, see "Managing Finder Preferences" on page 164.) Check the Commands pane of Finder preferences and make sure Restart and Shut Down are not selected.

Note: Login Window settings are available only for computer lists.

To disable the Restart and Shut Down buttons:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more accounts.
4. Click Login.
5. Click Login Window and set the management setting to Always.
6. Deselect the "Show Restart" and "Show Shut Down" buttons in Login Window.
7. Click Apply Now.

Using Hints to Help 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 displays the hint you created.

If a password hint has been created for a local user, the hint is always displayed after three failed attempts, even if Show Password Hint is not selected. Password hints are not used for network user accounts.

To show a password hint:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more accounts.
4. Click Login.
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.

Enabling Multiple Simultaneous Users on a Client Computer

With Fast User Switching, more than one account is available at the same time on a single computer. The list of current active (authenticated) accounts appears in a menu on the right side of the Finder menu bar; you switch to a different account by choosing it. A user must authenticate to switch to his or her account, but the previous user does not have to log out first.

Fast User Switching can be convenient for computers used by small, consistent groups.

To enable Fast User Switching:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more accounts.
4. Click Login.
5. Click Options and set the management setting to Always.
6. Select "Enable Fast User Switching" to allow users to use this feature. Deselect this option to disable it.
7. Click Apply Now.

Enabling Automatic Logout for Idle Users

You can reduce the load on your servers and help keep user accounts more secure by automatically initiating logout after a period of inactivity. When the set amount of time has passed, the user is logged out and returned to the login window.

Note: This feature is for clients running Mac OS X version 10.3 and later.

To log a user out automatically:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Click the Computer Lists button and select one or more accounts.
4. Click Login.
5. Click Options and set the management setting to Always.
6. Select "Log out users after" and enter the number of minutes of inactivity to wait before logging out.
7. Click Apply Now.

Enabling the Use of Login and Logout Scripts

You can use login scripts to perform a set of actions whenever a user logs in or logs out. Because login or logout scripts run as root, they are very powerful. Test your scripts to ensure that they do not negatively impact system settings or damage user files. You can add a login script to a computer in two ways. You can add a LoginHook to a specific computer, or you can apply a login script to a computer list using Workgroup Manager.

When enabling the use of login and logout scripts, you can set a trust value for the client. Trust values determine the required level of authentication before a client will trust a server enough to run its scripts. Most trust values directly correlate to LDAP security policy settings you configure in Directory Access. The trust value of DHCP correlates not to a security policy but rather to whether Directory Access is configured to use a DHCP-supplied LDAP server. The trust value of Authenticated requires you to set up trusted binding to an LDAP directory.

For more information about how to use Directory Access to enable LDAP security policies, using DHCP-supplied LDAP, or setting up trusted binding, see the Open Directory administration guide.

The following table lists valid trust values and describes their requirements. The table is in increasing trust order, where the bottommost entry requires the highest level of trust.

Trust value name	Requirements
Anonymous	The client trusts any directory domain server.
DHCP	Select "Add DHCP-supplied LDAP servers to automatic search policies" in Directory Access.
Encryption	Select "Encrypt all packets (requires SSL or Kerberos)" in Directory Access.
Authenticated	Set up trusted binding between the client computer and the LDAP directory.
PartialTrust	Select "Digitally sign all packets (requires Kerberos)" in Directory Access. Most Active Directory nodes support PartialTrust and not FullTrust.
FullTrust	Select "Block man-in-the-middle attacks (requires Kerberos)" and "Digitally sign all packets (requires Kerberos)" in Directory Access.

To set the minimum required trust level, you set a client setting called MCXScriptTrust. If the client's MCXScriptTrust setting is an equal or lower level of trust than the actual trust value, the client will trust the server and run its login and logout scripts. If the client's MCXScriptTrust setting is a higher level of trust than its actual trust value, the client will not trust the server and will not run its scripts. The default trust value is FullTrust.

To enable the use of login or logout scripts:

1. Log into the user's computer locally or use Apple Remote Desktop.
2. Open the Sharing pane of System Preferences.
3. Click the lock to authenticate, and click Edit.
4. If the local hostname contains any special nonalphabetical or nonnumeric characters, including spaces, dashes, and underscores, remove the special characters and click OK.

   For example, change local hostnames like "Anne-Johnson's-Computer" to "AnneJohnsonsComputer".
5. Optionally, determine the current trust level by entering the following command in Terminal:

   ```
   dscl localhost -read /LDAPv3/www.apple.com
        dsAttrTypeStandard:TrustInformation
   ```

   Replace `www.apple.com` with the address of your LDAP directory. Running this command displays a line similar to the following:

   ```
   TrustInformation: Authenticated FullTrust
   ```

   In this example, the current trust level is FullTrust. The trust level is also Authenticated. When two trust levels are listed, the higher trust level takes precedence.
6. Set the "EnableMCXLoginScripts" key in ~root/Library/Preferences/com.apple.loginwidow.plist to TRUE. Type the following command in Terminal:

   ```
   sudo defaults write com.apple.loginwindow EnableMCXLoginScripts -bool TRUE
   ```
7. To change the trust value from FullTrust, set the "MCXScriptTrust" key in ~root/Library/Preferences/com.apple.loginwidow.plist to a valid trust value. For example, enter the following command in Terminal:

   ```
   sudo defaults write com.apple.loginwindow MCXScriptTrust -string
        PartialTrust
   ```

   This command sets the trust value to `PartialTrust`. To set other trust values, replace `PartialTrust` with other trust values. If you enter an invalid trust value, the trust value is reset to FullTrust.

   Whenever you enable login and logout scripts or change the trust value, you should readd login and logout scripts in Workgroup Manager. For more information about how to use Workgroup Manager to add login and logout scripts, see "Running a Login or Logout Script".

Running a Login or Logout Script

You can only run login and logout scripts on computer lists. Before adding scripts to run, you need to enable using login and logout scripts on the clients. If you change the trust level for clients, you should readd your scripts. For instructions on enabling login and logout scripts on clients and for more information about trust levels, see "Enabling the Use of Login and Logout Scripts" on page 181.

You cannot run scripts that are larger than 30 KB.

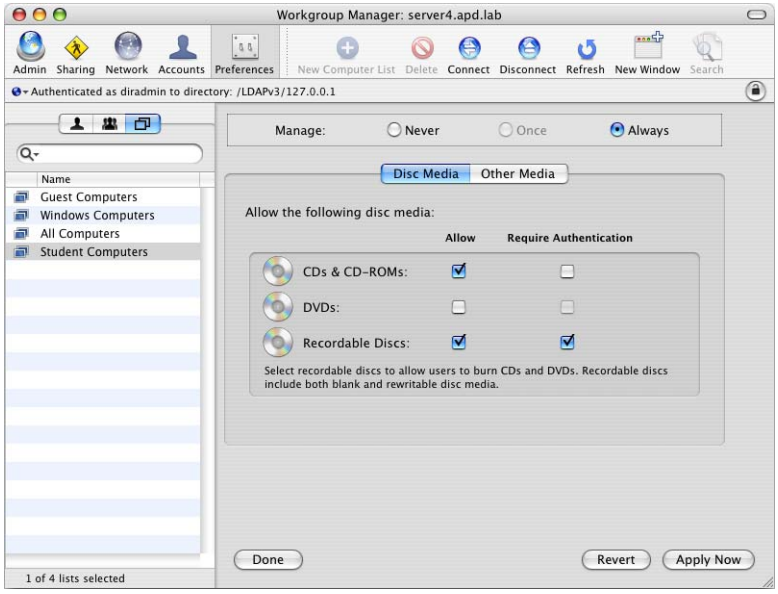
To add login or logout scripts:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more computer lists.
4. Click Login and click Scripts.
5. Set the management setting to Always.
6. Select Login Script or Log-Out Script. In the dialog that appears, locate your script and click Open.
7. 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).



The table below describes what you can do with the settings in each Media Access pane.

Media Access preference pane	What you can control
Disc Media	Settings for CDs, DVDs, and recordable discs (for example, a CD-R, CD-RW, or DVD-R). Computers without appropriate hardware are not affected by these settings.
Other Media	Internal hard disks, and external disks other than CDs or DVDs

Controlling Access to CDs, DVDs, and Recordable Discs

If a computer can play or record CDs or DVDs, you can control whether users can access items (music, movies, and so on) on these discs. You cannot permit access to only certain discs or to specific items on a disc.

If a computer has the appropriate hardware, you can control whether users can "burn" discs—that is, 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.

To control access to disc media:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Media Access.
5. Set the management setting to Always. This setting applies to all Media Access preference options.
6. Click Disc Media and select the desired options.
7. Click Apply Now.

Controlling Access to Hard Drives and Disks

You can control access to internal or external disk drives such as floppy disk drives, Zip drives, and FireWire drives.

Note: Behavior for internal hard disks may vary slightly between clients running Mac OS X 10.2 (Jaguar) and 10.3 (Panther). For consistent results, set access privileges for internal disks and partitions on individual clients by using Ownership and Permissions settings in the Finder.

To restrict access to internal and external disks:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Media Access.
5. Set the management setting to Always. This setting applies to all Media Access preference options.
6. Click Other Media and select desired options.

   If you select the Read-Only checkbox, users can view the contents of a disk but cannot modify it or save files on it.
7. Click Apply Now.

Ejecting Items Automatically When a User Logs Out

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 automatically eject removable media when a user logs out.

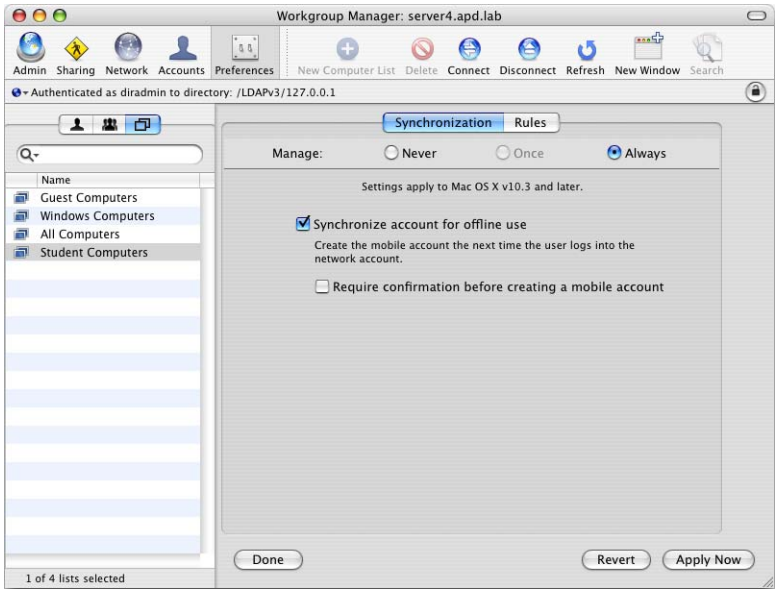
To eject removable media automatically:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Media Access.
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 Mobility Preferences

If a user requires a mobile account, you can specify one to be created for the user automatically during their next login.



The table below describes what you can do with the settings in each Mobility pane.

Mobility preference pane	What you can control
Synchronization	Whether to create mobile accounts and whether their mobile accounts should be automatically enabled when users log in
Rules	The folders you want to synchronize at login and logout, or in the background, and how frequently to synchronize folders in the background

For planning information and other considerations with mobile accounts, see Chapter 8, "User Management for Portable Computers."

Creating a Mobile Account

You can use Workgroup Manager to create a mobile account automatically when a user logs in. You can also allow the user to choose whether to access computers using a network account or to enable a mobile account on that computer. When you create or enable a mobile account, a local home folder is created for the user at first login.

To create a mobile account using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select a user account, group account, or computer list, and then click Preferences.

When you enable creating mobile accounts for a group account, when individual users log in with that workgroup, they are given individual mobile accounts. Similarly, if you enable creating mobile accounts for a computer list, when individual users log in using a computer on that list, they are given individual mobile accounts for that computer.

4 Click Mobility.

5 Click Synchronization and select Always.

6 Select "Synchronize account for offline use."

7 Select "Require confirmation before creating a mobile account" if you want to allow the user to decide whether or not to enable a mobile account at login.

If this option is selected, the user sees a confirmation dialog when logging in. The user can click Yes to create a local home folder and enable the mobile account, or click "Not now" to log in as a network user without enabling the mobile account. The user can also click Never to log in as a network user and not see the confirmation dialog again (except by holding down the Option key during login).

8 Click Apply Now.

Changes are applied to a mobile account the next time the client computer connects to the network.

Note: When a mobile account is enabled, it appears in the login window and in the Accounts pane of System Preferences with the label Mobile. When the account is selected in the Accounts pane, most settings appear dimmed.

Preventing the Creation of a Mobile Account

There are two ways to prevent the creation of mobile accounts. You can choose not to show Accounts in System Preferences as described in "Managing Access to System Preferences" on page 197. You can also prevent the creation of mobile accounts by managing Mobility preferences.

If you do not manage Mobility preferences and you allow the user to access the Accounts pane of System Preferences, network users can create their own mobile accounts.

If a user previously created his or her mobile account, he or she still has a local home folder after removing the account from the directory domain. You can delete the local home folders to save hard disk space. For instructions on deleting the local home folders, see "Removing Mobile Accounts from Client Computers" on page 188.

To prevent the creation of mobile accounts by managing Mobility preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Mobility.
5. Click Synchronization.
6. Set the management setting to Always.
7. Deselect "Synchronize account for offline use."
8. Click Apply Now.

Removing Mobile Accounts from Client Computers

If a user no longer requires a mobile account, you can delete the individual account on the client computer. When you delete the account, you can also delete or archive the user's local home folder. To delete a mobile account, you must log in to the client computer using an account other than the mobile account. You also need to know the name and password of an administrator account on the client computer. You cannot use Workgroup Manager to remove the account remotely.

Removing the account from the client computer changes the user's account type from a mobile account to a network account.

To remove a mobile account from a client computer:

1. Open System Preferences on the client computer.
2. Click Accounts, and then click the lock and authenticate as the local administrator, or as a domain administrator with permission to manage the computer list the client computer belongs to.
3. Select the mobile account you want to remove.

   The mobile account should have the word "Mobile" listed in the Type column.
4. Click the Delete (–) button.
5. Choose OK to archive the user's home folder, or click Delete Immediately.

Choosing Folders to Synchronize at Login and Logout, or in the Background

You can use Workgroup Manager to choose which folders to synchronize at login and logout, or in the background for users with mobile accounts. You can also choose not to synchronize specific folders.

Login and logout synchronization should be carefully managed because a user's login and logout is delayed while files are synchronizing. Using background synchronization can also cause users to load outdated files from the network, especially when synchronization is set to occur at long intervals. Also, you cannot synchronize ~/Library in the background.

For detailed information about things you should consider when choosing folders to synchronize and how to synchronize them, see "Strategies for Synchronizing Content" on page 120.

To choose folders to synchronize at login and logout, or in the background:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Mobility.
5. Click Rules, and then click Login & Logout Sync or Background Sync.
6. Set the management setting to Always.
7. To add folders, click the Add (+) button for the "Synchronize ..." list, enter the path to the folder that you want to synchronize, and press Enter.

   Typically, you want to synchronize a folder in your user's home folder. Precede the folder with ~/ to denote the location of the synchronized folder within the user's home folder. For example, to synchronize the user's Documents folder, enter ~/Documents.
8. Alternatively, you can click the Browse (...) button for the "Synchronize ..." list to browse on the server for a folder to add.

   Because you are browsing the server currently running Workgroup Manager, you could choose a folder that is not located in the user's account. If you choose a folder that doesn't exist in the user's account, no files are synchronized.
9. To choose not to synchronize specific files or folders, use the Add (+) button or Browse (...) button to add items to the "Skip items that match any of the following" list.

   To filter for specific items, click the Match field entry for any list item. This allows you to further specify your search.

10 To add your synchronized folders to the folders that the user selects for synchronization, select "Merge with user's settings."

If you choose to synchronize the same folder in Workgroup Manager as the user chooses in the Accounts pane of System Preferences, merging will make your synchronization settings take precedent. If you do not select "Merge with user's settings," the folders you choose to synchronize will replace those chosen by the user.

When used in conjunction with Once, merging with the user's settings is useful for adding new folders to synchronize, without disrupting the folders the user set to synchronize.

11 Click Apply Now.

Setting the Background Synchronization Frequency

You can change the frequency with which background folders synchronize for mobile accounts. By default, background folders synchronize every 20 minutes. You can set frequencies from five minutes to sixty minutes.

Carefully set the background synchronization frequency. If you set it to a short interval and you have many concurrent users, you might overload the server. In this situation, the server could become backlogged by the frequent, continual comparing of file modification dates. If you set the frequency to a very long interval, you run a higher risk of users loading older, outdated files. If users save files and log off before the background files synchronize, when the users load the same file on another computer, they may get either an older synchronized file or no file at all.

To set the frequency for synchronizing background folders:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Mobility.

5 Click Rules, and then click Background Sync. Ensure that the management setting is Once or Always.

6 Click Options and set the management setting to Always.

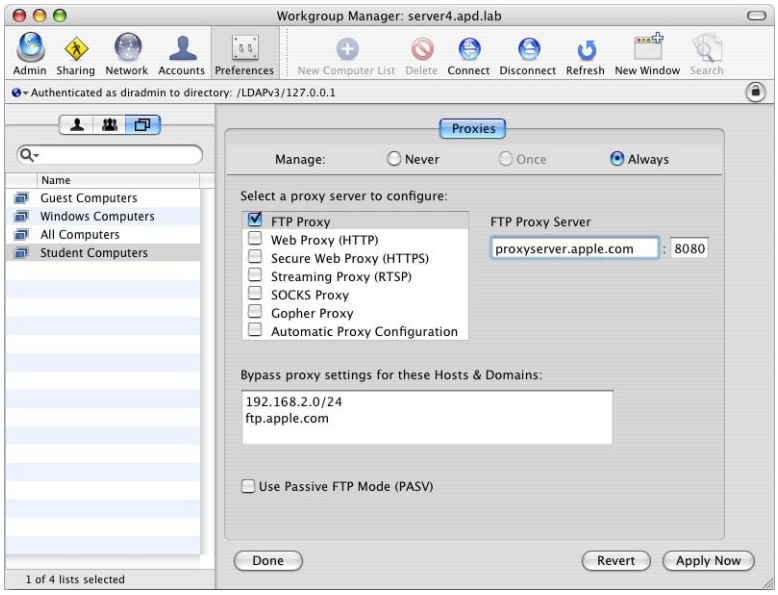
7 Click Every and drag the slider to set the frequency for background folder synchronization. If you want background folders to synchronize only when users choose to, click Manually.

The default frequency is 20 minutes. The frequency you set also affects any folders your users configure to synchronize automatically.

8 Click Apply Now.

Managing Network Preferences

Network preferences let you select and configure proxy servers that can be used by users and groups. You can also specify hosts and domains for which to bypass proxy settings. This has the advantage of providing a customized browsing experience for the managed users and groups.



Configuring Proxy Servers by Port

You can configure specific types of proxies for a user or group to access and specify the exact port. The types of proxy servers modifiable individually are: FTP, Web (HTTP), Secure Web (HTTPS), Streaming (RTSP), SOCKS, Gopher, and Automatic Proxy Configuration.

The server administrator manages which users or groups get these proxies and specifies the proxy they are allowed to access in the Preferences pane of Workgroup Manager. Only one proxy server per type can be specified for a user or a group.

To configure proxy servers for a user or a group:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Network.
5. Set the management setting to Always.

6 Select the specific type of proxy you want to configure (FTP, Web, and so on).

7 Specify a URL and port of the form: proxyserver.apple.com:8080.

8 Click Apply Now.

Allowing Users to Bypass Proxy Servers for Specific Domains

When managing Network preferences for users, you can allow users to bypass your proxy settings for specific hosts or domains. By bypassing the proxy server, the user connects directly to the specified addresses.

If you haven't already set the management settings of Network preferences to Always and enabled a proxy server, you need to do so before choosing which hosts and domains to bypass.

To choose the domains that users can access directly:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Network.

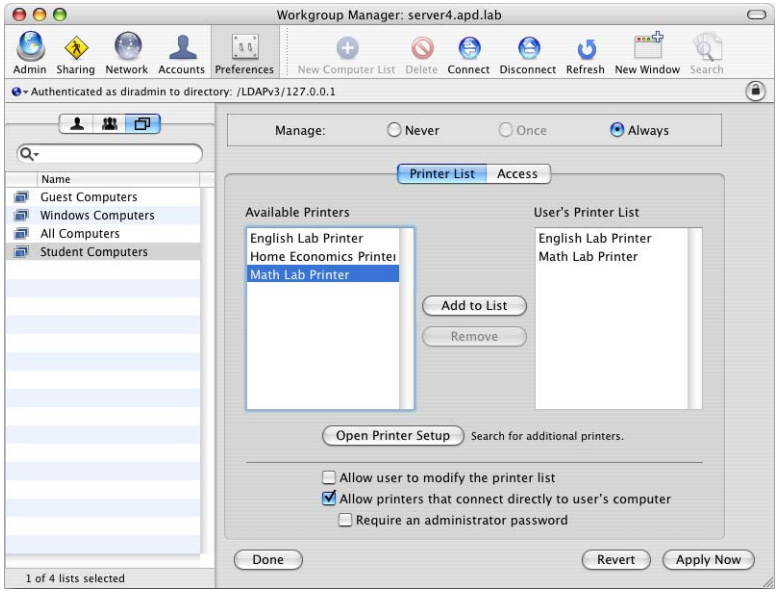
5 In the "Bypass proxy settings for these Hosts & Domains" field, enter the addresses of the hosts and domains that you want users to be able to connect to directly. To enter multiple address, separate the subnet masks with newlines, spaces, semicolons, or commas. There are several ways to enter addresses:

- A subdomain or fully qualified domain name (FQDN) of a target server, such as server1.apple.com or store.apple.com.
- The specific IP address of a server, such as 192.168.2.1.
- A domain name, such as apple.com. This bypasses apple.com, but not any subdomains such as store.apple.com.
- An entire website, including all subdomains, such as *.apple.com.
- A subnet in Classless Inter-Domain Routing (CIDR) notation. For example, if you wanted to add a subnet of 192.168.2.x, you would name that view 192.168.2.0/24. For a detailed description of subnet masks and CIDR notation, see the network services administration guide.

6 Click Apply Now.

Managing Printing Preferences

Use Printing preferences to create printer lists and manage access to printers.



The table below describes what the settings in each Printing pane can do.

Printing preference pane	What you can control
Printer List	Available printers, and the user's ability to add printers or access a printer connected directly to a computer
Access	The default printer, and access to specific printers

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 actual 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. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Printing.

5 Set the management setting to 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 Printer Setup Utility.

Select a printer in the Available Printers list, and 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 Printer Setup and add the printer to Printer Setup Utility's printer list.

8 Click Apply Now.

Preventing Users from Modifying the Printer List

You can prevent a user from changing the list of available printers (by adding or removing printers).

To restrict access to the printer list:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Printing.

5 Set the management setting to Always. This setting applies to all Printing preference options.

6 Click Printer List.

7 To require an administrator to modify the printer list, deselect the "Allow user to modify the printer list" checkbox.

8 Click Apply Now.

Restricting Access to Printers Connected to a Computer

In some situations, you might want only certain users to print to a printer connected directly to their computer. For example, if you have a computer in a classroom with a printer attached, you can reserve that printer for teachers 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 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Printing.

5 Set the management setting to Always.

This setting applies to all Printing preference options.

6 If it's a network printer you want the client computer to have access to, click Printer List, select the printer, and click "Add to List."

7 If you don't want users to access local printers, deselect "Allow printers that connect directly to the user's computer." To require an administrator password in order to use the printer, select "Require an administrator password."

8 Click Apply Now.

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 print dialog.

To set the default printer:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Printing.

5 Set the management setting to Always. This setting applies to all Printing preference options.

6 Click Access.

7 Select a printer in the user's printer list, and 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 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Printing.

5 Set the management setting to Always. This setting applies to all Printing preference options.

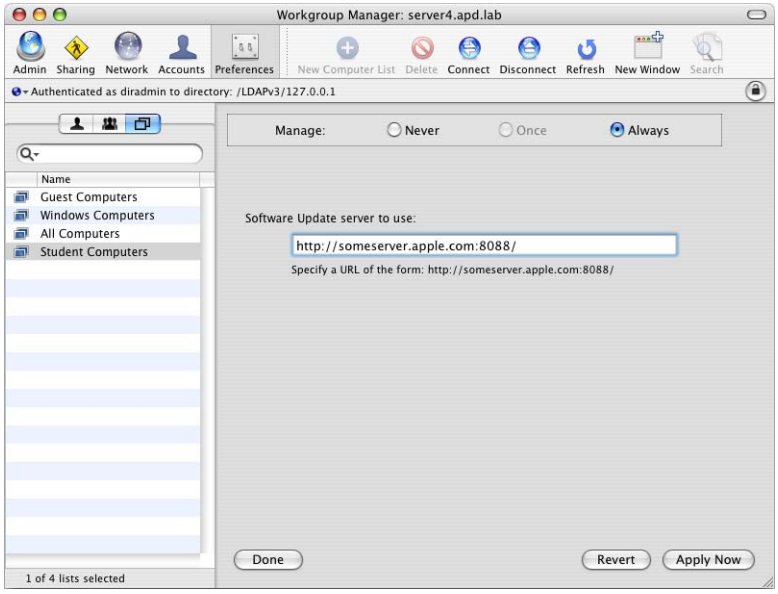
6 Click Access.

7 Select a printer in the User's Printer List, and then select "Require an administrator password."

8 Click Apply Now.

Managing Software Update Preferences

With Mac OS X Server, you can create your own Software Update server to control the updates that are applied to specific users or groups. This is advantageous because it reduces external network traffic while also providing more control to server administrators. By configuring the Software Update server, server administrators can choose, which updates to provide.



To manage access to Software Update servers:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Software Update.

5 Set the management setting to Always.

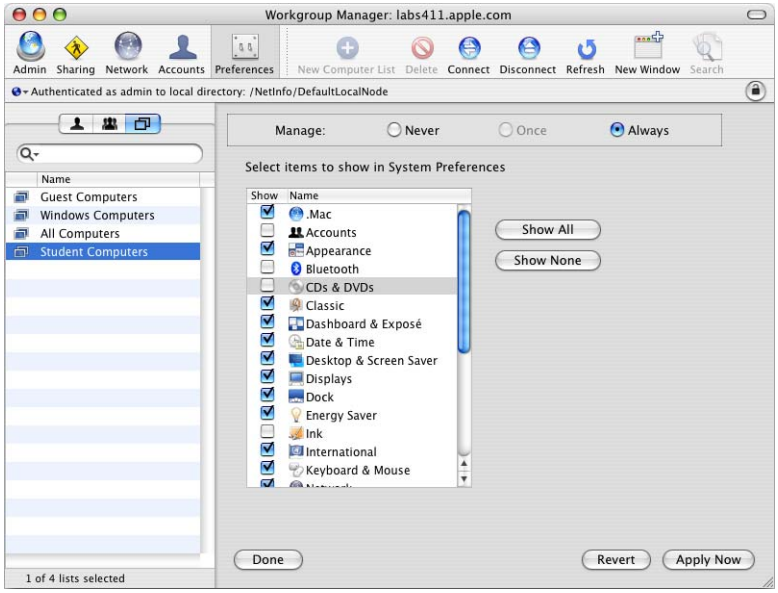
6 Specify a URL of the form: http://someserver.apple.com:8088/.

7 Click Apply Now.

Managing Access to System Preferences

You can specify which preferences are displayed in System Preferences. If a user can display a particular preference, it does not necessarily mean that the user can modify that preference. Some preferences, such as Startup Disk preferences, require an administrator name and password before a user can modify its settings.

The preferences that appear in Workgroup Manager are those installed on the computer you're currently using. If your administrator computer is missing any preferences that you would like to disable on client computers, you should either install the applications related to those preferences, or use Workgroup Manager on a computer that includes those preferences.



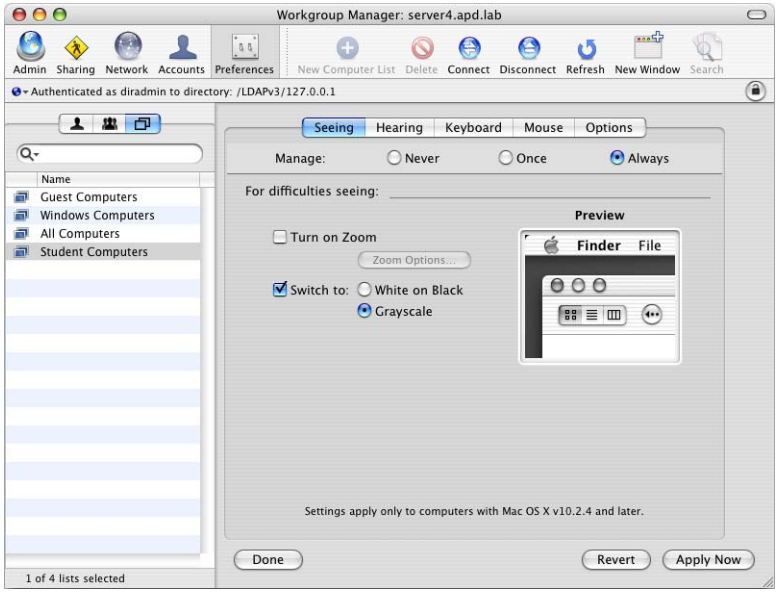
To manage access to System Preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click System Preferences.
5. Set the management setting to Always.
6. Deselect the Show checkbox for each item you don't want to display in a user's System Preferences.
7. Click Apply Now.

Managing Universal Access Preferences

Universal Access settings can help improve the user experience for certain users. For example, if a user is a person with a disability, has difficulty using a computer, or wants to work in a different way, you can choose settings that enable the user to work more effectively. Using Workgroup Manager, you may want to set up and manage Universal Access settings for specific workgroups or computers dedicated to users with special needs.



The table below describes what the settings in each Universal Access pane can do.

Universal Access preference pane	What you can control
Seeing	The visual display and desktop zooming
Hearing	The visual alert for users
Keyboard	How the keyboard responds to keystrokes and key combinations
Mouse	How the pointer responds, and whether users can use the numeric keypad instead of a mouse
Options	Shortcut key combinations, the use of assistive devices, and whether the computer reads text in the Universal Access preference pane

Adjusting the User's Display Settings

Workgroup Manager's Seeing preferences allow users to adjust the appearance of the screen. The user can easily zoom in or out on the desktop using keyboard shortcuts (specific key combinations). Changing to a grayscale or white-on-black display can make it easier to read text on the screen.

Note: If display settings are managed once, users can toggle between the zoom or color options using keyboard shortcuts. If the management setting is Always, users cannot toggle between options.

To manage Seeing preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Universal Access.
5. Click Seeing, and then select a management setting (Once or Always).
6. Make changes as desired.
7. To fine-tune zoom settings, click Zoom Options.

   Use the sliders to set a Maximum Zoom and Minimum Zoom.

   To show a preview area, select "Show preview rectangle when zoomed out."

   To improve the appearance of zoomed graphics, deselect "Smooth images."
8. Click Apply Now.

To further customize the user's display, you can use Finder View preferences to control the size of icons in Finder windows and use Dock Display preferences to enlarge or magnify icons in the user's Dock.

If you plan to manage dedicated computers, you may be able to use Display preferences to change the resolution of your display and the number of colors your display uses. If you want to keep the local Display preferences as you set them, you may want to remove the Display item from the list of available System Preferences using Workgroup Manager's Applications preference.

To allow the use of an assistive device on a specific computer, such as a screen reader, click Preferences, select a computer list, click System Preferences, click Universal Access, click Options, click Always, and select "Enable access for assistive devices."

Setting a Visual Alert

If users have trouble hearing a computer's alert sounds (for example, the sound played when new mail arrives or an error occurs), you can flash the screen as an alternative.

To set a flashing alert:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Universal Access.
5. Click Hearing, and then select a management setting (Once or Always).
6. Select "Flash the screen whenever an alert sound occurs."
7. Click Apply Now.

Adjusting Keyboard Responsiveness

If users have difficulties pressing multiple keys at once, you can use the Sticky Keys feature to allow the keyboard to recognize a sequence of individual keystrokes as a key combination. The computer can display each keystroke on the screen, and then respond with an alert when the key combination is complete.

Note: If you enable Universal Access Shortcuts, a user can press the Shift key five times to turn Sticky Keys on or off.

If the keyboard is too responsive for some users, causing problems with repeated keystrokes, you can use Slow Keys to increase the delay in response to a pressed key. The computer can respond to pressed keys with a "click" sound to provide some feedback to the user.

To set how the keyboard responds to keystrokes:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Keyboard, and then select a management setting (Once or Always).

6 Select On to activate Sticky Keys.

To turn off the key combination alert, deselect "Beep when a modifier key is set."

To turn off onscreen display of keystrokes, deselect "Show pressed keys on screen."

If these options are not selected, users may not easily know when a key combination is in progress or completed.

7 Select On to activate Slow Keys.

8 If you don't want the computer to respond to keystrokes with a click, deselect "Use click key sounds."

9 Move the slider to adjust the amount of delay between when a key is pressed and when the computer accepts it.

10 Click Apply Now.

Adjusting Mouse and Pointer Responsiveness

If users have difficulties using a mouse or prefer not to use a mouse, the Mouse Keys feature allows them to use the numeric keypad instead. Keys on the numeric keypad correspond to directions and mouse actions, so the user can move the pointer and hold, release, or click.

Note: If you enable Universal Access Shortcuts, a user can press the Option key five times to turn Mouse Keys on or off.

If the pointer moves too quickly for some users, you can adjust how soon the pointer begins to move and how fast it moves.

To control mouse and pointer settings:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Mouse, and then select a management setting (Once or Always).

6 Select On to activate Mouse Keys.

7 To control how long it takes for the pointer to begin moving, adjust the Initial Delay slider.

8 To control how fast the pointer moves, adjust the Maximum Speed slider.

9 Click Apply Now.

Enabling Universal Access Shortcuts

Universal Access Shortcuts are key combinations that activate an available access feature, such as zooming in on the screen or turning on Sticky Keys. If you choose not to allow Universal Access shortcuts, users may not be able to use features such as Zoom and may not be able to turn off activated features such as Sticky Keys.

To allow Universal Access Shortcuts:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Options, and then select a management setting (Once or Always).

6 Select Allow Universal Access Shortcuts.

7 Click Apply Now.

Allowing Devices for Users with Special Needs

You can allow managed users to turn on assistive devices, such as a text reader.

To allow assistive devices:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and that you are authenticated for it.

To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

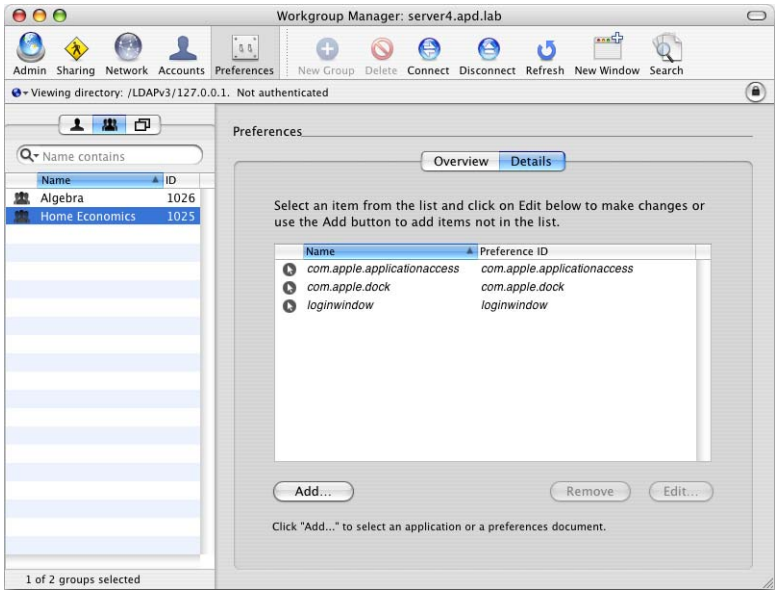
5 Click Options, and then select the Always management setting.

6 Select "Enable access for assistive devices."

7 Click Apply Now.

Using the Preference Editor with Preference Manifests

Workgroup Manager includes a preference editor, which you can use to control any Mac OS X application or utility developed using Apple standard conventions for handling preferences. You can also use it to manage preferences that are not configurable in Workgroup Manager's main preferences interface. Like the main preferences interface, you can use the preference editor to manage preferences for users, groups, and computer lists.



Some application developers provide preference manifests, which make it easier to read and modify the application's preferences using the preference editor. You can edit an application's preference key values even if the application doesn't provide a preference manifest.

A preference manifest simplifies modification of preferences by replacing cryptic preference key names with more easily read names. For example, in Safari you can enable displaying the status bar by setting Safari's ShowStatusBar key to true. If you save this key in the Often group, the status bar can be disabled by the user for their current session, but it automatically reenables in every new session. For applications without preference manifests, you have to work with key value names that are not always as well described as ShowStatusBar.

Preference manifests may be stored in an application package (a .manifest file in the package's /Contents/Resources/ folder), or they may be standalone files. If they exist for an application, the preference editor loads them when you add the application to the preference editor application list. Preference manifests provide names and descriptions of keys that are honored by an application, and tell you how to set them.

Adding an Application to the Preference Editor's Application List

Before editing keys for an application, you must add the application to the preference editor's application list. To add an application to the list, you can either add the application itself or you can add its preference file, located in ~/Library/Preferences/.

To add an application to the preference editor's application list:

1. In Workgroup Manager, click Preferences, and then click Details.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Click Add.
5. Select either an application located in /Applications or a .plist file located in ~/Library/Preferences/, and click Add.

   If the application provides a preference manifest, it appears in the list unitalicized. Applications without preference manifests appear in italics.

   When you add an application by selecting its .plist file from ~/Library/Preferences/, the selected accounts also inherits your current preferences. With this ability to directly add the preference file, you can manage any application that uses Mac OS X preferences.

Editing an Application's Preferences with the Preference Editor

You can use Workgroup Manager's preference editor to edit and manage application-specific preferences. An application that follows Apple standard conventions for handling preferences should respect the settings in a preference manifest. For applications without preference manifests, you should test your settings to ensure they produce the desired results.

Before using the preference editor to manage an application's preferences you must add the application to the preference editor's application list. For instructions on adding an application to the application list, see "Adding an Application to the Preference Editor's Application List" on page 204.

To edit an application's preferences:

1. In Workgroup Manager, click Preferences, and then click Details.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Select an item in the application list and click Edit.
5. Click the disclosure triangles to locate the keys you want to modify.

   The preference file editing screen divides keys by management frequency. Always and Once are similar to choosing Always and Once in Workgroup Manager's main preferences interface. Often is only available in the preference editor. Always sets a preference and does not allow the user to modify the preference. Once sets a preference but allows the user to change that preference and retain his or her saved preference. Often allows users to modify their preferences, but they revert to your managed settings every time users begin a new session.

   Always may still allow users to modify preferences. For this reason, Often is usually a better choice for making persistent preference changes.
6. Select a key to modify. Click the up and down arrows to the right of the key's type or value to change the key's current settings.

   If you change the type to a setting that is not by default enabled by the preference manifest, the preference file editing screen indicates the mismatch with an arrow icon. This does not prevent you from changing the key's type.
7. If you want to add a key to the application's preferences file, click New Key, enter the exact name of the key, and select the key's type and value.

   Be very careful when adding keys to preference files. You need to know the exact name of the key and the types of values it supports. When you add new keys, you should always test your additions to make sure they work as expected.
8. Click Apply Now, and then click Done.

Disabling Management of an Application's Preferences Using the Preference Editor

If you want to disable management of an application's preferences through the preference editor, remove the application from the preference editor's application list. This does not delete an application's preference manifest or the application's preferences file.

To disable managment of an application's preferences:

1. In Workgroup Manager, click Preferences, and then click Details.
2. Make sure the correct directory is selected and that you are authenticated for it.

   To switch directories, click the globe. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
3. Select one or more users, groups, or computer lists.
4. Select the application or bundle ID (this can only be done one application at a time).
5. Click Remove or click Clear.

   Remove is replaced by Clear for applications that cannot be removed from the preference editor, such as Safari.

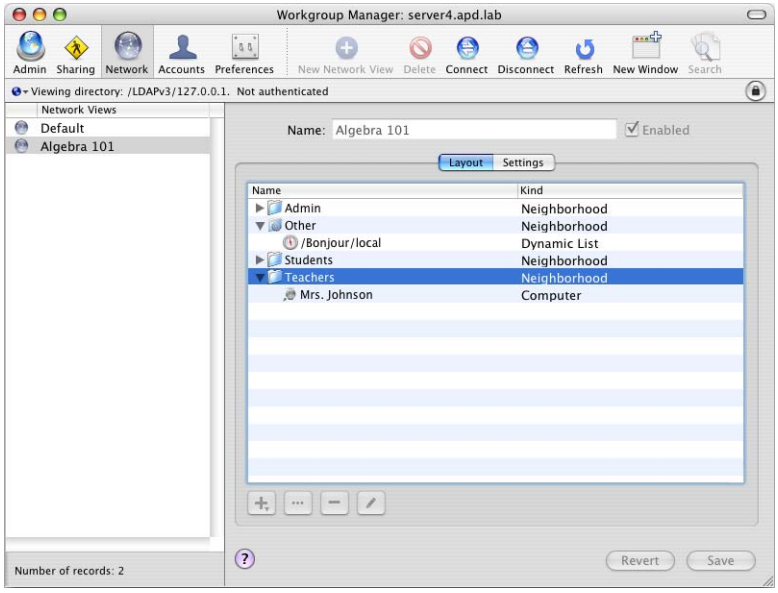
Managing Network Views

11

This chapter provides information about managing the network resources that users can view and access.

By using network views, you can control what is seen by users of a particular computer with Mac OS X version 10.4 or later installed when they click the Network icon in the sidebar of a Finder window, or when they choose Go > Network in the Finder.

You use the Network pane in Workgroup Manager to create and manage network views.



About Network Views

A network view is a list of network resources that you customize to enhance a user's browsing and resource discovery experience. You can add network resources to what a user already sees, or specify exactly which items a user sees. You can customize network views for a single computer, a group of computers, or an entire subnet.

You can create network views that contain one or more of these components:

- A *neighborhood,* which is a collection of network resources that are grouped for easy access. A neighborhood looks like a folder in the network view. A neighborhood can contain computers, other neighborhoods, and dynamic lists.
- A *computer* is any computer on the network. You can add computers directly to a network view or you can add them to a neighborhood within a network view.
- A *dynamic list* gives you the ability to automatically generate a list of network resources for display inside a neighborhood. For example, you can define a neighborhood called Marketing and show within it any active computer on the marketing subnet.

Types of Network Views

You can create three types of network views:

- *Named view.* A named view is visible on only specific client computers. You associate a view with a computer either when adding or editing the computer record in the directory domain, or by naming the view using an Ethernet address, an IP address, or a subnet string. The directory domain in which the named view is stored must be in the client computer's search policy.
- *Default view.* A view named Default is visible on a client computer if the directory domain in which the view is stored is in its search policy and no named view has been assigned to the computer.
- *Public view.* A view named Public is visible on a client computer if the directory domain where the view is stored isn't already providing a network view for the computer. The directory domain can be any directory domain that a computer is configured to access, on or off its search policy.

  If a Public view isn't found in any such directory domain but a Default view is, the Default view is displayed.

Administering Network Views

This section describes how to define network views, including how to specify their layout and associate client computers with them.

Creating a Network View

When you create a network view, you define neighborhoods and include computers and dynamic lists with the view. You also list the client computers that use the view.

To create a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which you want the view to reside.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. Choose Server > New Network View or click New Network View in the toolbar, select the type of view you want to create, and click Create.

   For more information about the various types of views, see "Types of Network Views" on page 208.
5. If you're defining a named view, enter a name for the view in the Layout pane.

   If you want the named view to be used by all computers in a subnet, name the view using the subnet mask in Classless Inter-Domain Routing (CIDR) notation. For example, if you wanted your subnet of 192.168.2.x to use a particular view, you would name that view 192.168.2.0/24. For a detailed description of subnet masks and CIDR notation, see the network services administration guide.

   If you want the named view to be visible on a particular computer, you can name the view using either the client computer's IP address or Ethernet address. You can also add the computer as a client for the view using its IP or Ethernet address. You can also associate the view with specific computers by editing individual computer records.

   For more information about how to associate views with computers, see "Naming a Network View to Associate It with a Computer" on page 217 and "Adding Network View Clients" on page 217.
6. In the Layout pane, add neighborhoods, computers, and dynamic lists to the view.

   For instructions, see "Adding Neighborhoods to Network Views" on page 211, "Adding Computers to Network Views" on page 212, and "Adding Dynamic Lists to Network Views" on page 215.
7. Finalize the network view hierarchy. Drag elements up or down in the list in the Layout pane to add them to neighborhoods or remove them from neighborhoods.

Items in the list are displayed alphabetically, as they are when viewed in a client's Finder. If your network view contains a mixture of dynamic lists and computers, the computers contained within the dynamic lists and the computers you individually list will be mixed together and sorted alphabetically. Consider organizing views containing both dynamic lists and computers into neighborhoods. Displaying all resources within neighborhoods gives you the opportunity to assign a meaningful name to a collection of resources.

8 Set up client computer settings for the view using the Settings pane.

For instructions, see "Working with Network Views on Client Computers" on page 216.

9 If you want to make the network view visible immediately on client computers, click Layout, and then select the Enabled checkbox.

10 Click Save.

Renaming a Network View

Name your network views to help remind you of the type of network resources included in the view or of the clients associated with it.

Default and Public views should keep their automatically created names of "Default" and "Public." These are reserved names that should be not be changed. By changing their names, you effectively change them into named views, which must be associated with specific client computers. Additionally, you should not rename named views to "Default" or "Public" unless you want them to become Default or Public views.

To rename a network view:

1 Open Workgroup Manager, and click Network.

2 Click the globe to choose the directory domain in which the view resides.

3 Click the lock to authenticate as a domain administrator for the directory.

4 In the Network Views list, select the view you want to rename.

5 Type the new name in the Name field and press Enter.

6 Click Save.

Deleting a Network View

You can delete a network view so that no clients can use the network view.

> *Warning:* You cannot undo deleting a network view.

To delete a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory.
4. In the Network Views list, select the view you want to delete.
5. Click Delete in the toolbar or choose Server > Delete.
6. Click Delete.

Enabling or Disabling a Network View

You can disable a network view without deleting the network view or modifying the network view's layout or settings.

To enable or disable a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory.
4. In the Network Views list, select the view you want to disable.
5. Select or deselect Enabled to enable or disable the network view.
6. Click Save.

Adding Neighborhoods to Network Views

Neighborhoods enable you to group network resources in a logical manner and organize the presentation of your network resources. You can add any number of neighborhoods to a network view. In the network view, a neighborhood looks like a folder.

To add a neighborhood to an existing network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory.
4. In the Network Views list, select the view you want to work with.
5. In the Layout pane, click the Add (+) button and choose New Neighborhood.

If you want to add the neighborhood as a member of another neighborhood, first select an existing neighborhood before clicking Add. Alternatively, you can create the neighborhood and drag it on top of the existing neighborhood to make it a member of the existing neighborhood.

6 Type a name for the neighborhood and click Save.

Note: Finder cannot display neighborhood names of more than 255 characters.

Deleting Neighborhoods from Network Views

Deleting a neighborhood from a network view removes it from the list of resources visible in the view. It also removes all network resources that are members of the neighborhood. Be careful when deleting neighborhoods, because you do not receive any warning if there are resources in the neighborhood.

To delete a neighborhood from a network view:

1 Open Workgroup Manager, and click Network.

2 Click the globe to choose the directory domain in which the view resides.

3 Click the lock to authenticate as a domain administrator for the directory.

4 In the Network Views list, select the view you want to work with.

5 In the Layout pane, choose the neighborhood you want to delete.

6 Click the disclosure triangle to reveal everything in the neighborhood and confirm that you want to delete it and all its contents.

Drag neighborhood objects outside the neighborhood if you want to keep them associated with the view.

7 Click the Delete (–) button.

> ***Warning:*** If you click Delete in the toolbar or choose Server > Delete, you will delete the network view, not the neighborhood.

8 If you think you may have deleted objects inadvertently, click Revert. Otherwise, click Save.

Adding Computers to Network Views

You can add a computer to a network view only if the computer has a computer record in the directory domain where the network view resides. If you want to add a computer that does not have a record in the directory domain, you can add the computer to the directory domain while adding it to the network list.

A computer record may already exist if:

- The computer is managed using computer list preferences.
- The computer is already associated with another network view.

- The computer has been designated to use another network view in the directory domain.

Before adding a computer to the directory domain, ensure that it is not already in the directory domain. Although you can add the same computer to a directory domain multiple times, this can have unintended consequences. To display a list of the computers already added to the directory domain, choose Show Computers from the Add (+) pop-up menu. Double-click a listed computer to display its information.

To add a computer to a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view you want to work with, and make sure the Layout pane is visible.
5. Click the Add (+) button to add a computer to the network view. There are two ways to add computers after clicking Add:
   - Use an existing computer record by choosing Show Computers. Drag computers from the drawer into the Layout pane to add them to the network view. This is the preferred method for adding computers to network views because it prevents you from creating duplicate computer records and is usually faster than creating new computer records.
   - Create a new computer record by choosing New Computer. In the dialog that appears, enter information into the Name and URLs fields. In the Name field, type the name you want to use to identify the computer when it's displayed in the view. In the URLs field, type one or more URLs by which the computer can be reached. If you want to later add this computer as a client of a view, enter an Ethernet ID. You can also enter an Ethernet ID to specifically refer to a computer that has a dynamic URL address.
6. Alternatively, if the computer that you want to add has file sharing enabled, click the Browse (...) button to browse for it. Select the computer from the list and click Connect. This adds the computer to the network view. If the computer does not have a computer record in the directory domain using its computer name, the directory domain adds a new record for the computer.

   The server initiates a URL-based search, which looks for services with the standard file service types (AFP, SMB/CIFS, FTP, and NFS). You are able to browse through all the computers you would normally see under /Network. Select a computer from the list.
7. Click Save.

Editing Computers in Network Views

You can edit a computer record used in network views. This allows you to change the name, computer list, Ethernet ID, network view, URLs, comments or keywords.

To edit a computer in a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view you want to work with. You can edit computer records in both the Layout and Settings panes.
5. Double-click a computer record, or select a computer record and click the Edit (pencil) button.

   Alternatively, if the computer record is not listed, you can edit its directory entry by clicking Add (+) then clicking Show Computers. Double-click an entry in the sidebar.
6. Make changes in the edit dialog as appropriate.

   You can quickly change a computer's network view by choosing another network view from the Network View pop-up menu. You can also quickly associate a computer with a computer list by choosing a computer list from the Computer List pop-up menu.
7. Click Save.

Deleting Computers from Network Views

Deleting a computer from a network view removes it from the list of available resources within that network view.

To delete a computer from a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view you want to work with.
5. In the Layout pane, select the computer record you want to delete from the view. You may have to reveal the contents of neighborhoods, using the disclosure triangles, to see the computer in the list.
6. Click Delete (–).

> ***Warning:*** If you click Delete in the toolbar or choose Server > Delete, you will delete the network view, not the neighborhood.

7. If you think you may have deleted a computer inadvertently, click Revert. Otherwise, click Save.

Adding Dynamic Lists to Network Views

You can use dynamic lists to automate the display of network resources.

Mac OS X and Mac OS X Server can use Open Directory to discover network services, such as file servers, that make their locations known with AppleTalk, Bonjour, SLP, or SMB/CIFS service discovery protocols. You use Directory Access on the server hosting your network views to enable or disable the various service discovery protocols you may want to use to provide dynamic lists.

To add a dynamic list to a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view you want to work with.
5. In the Layout pane, click the Add (+) button and choose Add Dynamic List.
6. In the list that appears, select a service discovery location. You can select multiple locations by holding down the Command key while selecting them.

   The list displays available service discovery locations as: */protocol/neighborhood*. If you add a /protocol location, this adds all neighborhoods that use that protocol to the network view. If you add a /protocol/neighborhood location, this adds all the computers and subneighborhoods within that location to the network view.

   If the list doesn't include the service discovery location that you want to add, use Directory Access to enable the corresponding service discovery protocol.

   For additional information, see the Open Directory administration guide.
7. Click Add.
8. Click Save.

Deleting Dynamic Lists from Network Views

Deleting a dynamic list from a network view removes it from the list of available resources within that network view.

To delete a dynamic list from a network view:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view you want to work with.
5. In the Layout pane, select the dynamic list you want to delete from the view. You may have to reveal the contents of neighborhoods, using the disclosure triangles, to see the list.

You can delete more than one dynamic list at a time by holding down the Command key or the Shift key as you select lists.

6 Click Delete (–).

> ***Warning:*** If you click Delete in the toolbar or choose Server > Delete, you will delete the network view, not the neighborhood.

7 If you think you may have deleted a list inadvertently, click Revert. Otherwise, click Save.

Working with Network Views on Client Computers

Several techniques are available for setting up computers to display network views and controlling how views behave on client computers.

How a Computer Finds Its Network Views

When a Mac OS X computer starts up or when you use Directory Access to change search policy settings, the Mac OS X computer searches through the directories in its search policy. If it detects a computer record for itself in one of the directories and the computer record has a network view associated with it, it uses that view and stops searching.

If the computer doesn't find a computer record with an assigned network view, it searches through the directories in its search policy for a network view whose name matches one of the following criteria, in the order listed:

- The computer's Ethernet address
- The computer's IP address
- The computer's subnet string

If a network view matching one of these criteria is found, the computer uses that view and stops searching. But if no network view is found, the computer searches through directories in its search policy for a view named Default. The first Default view found is used.

The client computer first searches through all directories in its search policy. If it cannot find a suitable network view, the client computer then searches all directories it is configured to access, including those not in its search policy. For each directory domain, if it finds a Public network view, it displays it in a folder named after the server hosting the directory domain. If it doesn't find a Public view but does find a Default view in the directory domain, the Default view is displayed in a named folder.

Naming a Network View to Associate It with a Computer

Use one of these techniques to associate a named network view with a client computer:

- Name the view using a subnet identifier that includes the computer.
- Name the view using the computer's Ethernet address or IP address.
- Name the view something else and identify the view in a computer record for the computer.

To rename a network view and associate it with a computer record:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view.
5. Enter a new name for the network in the Name field and press Enter.

   If you want the named view to be used by all computers in a subnet, name the view using the subnet mask in Classless Inter-Domain Routing (CIDR) notation. For example, if you wanted your subnet of 192.168.2.x to use a particular view, you would name that view 192.168.2.0/24. For a detailed description of subnet masks and CIDR notation, see the network services administration guide.

   To associate a view with an IP address, name the view using an IP address. For example, name the view 192.168.2.1.

   To associate the view with a particular computer, name the view using the client computer's Ethernet address. For example, name the view 00:01:23:34:56:78.
6. Click Save.

   Make sure that the authentication search policy of the computer is configured to access the directory domain in which the view is stored.

Adding Network View Clients

You can associate a network view with computers by adding the computers to the clients list of the network view.

To add computers to the network view's client list:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view and click Settings.
5. Click the Add (+) button to add a computer as a client of the network view. There are two ways to add computers after clicking Add:

- Use an existing computer record by choosing Show Computers. Drag computers from the drawer into the Layout pane to add them to the network view. This is the preferred method for adding computers as network view clients, because it prevents you from creating duplicate computer records and is usually faster than creating new computer records.
- Create a new computer record by choosing New Computer. In the dialog box that appears, enter information into the Name, URLs, and Ethernet ID fields. In the Name field, type the name you want to use to identify the computer when it's displayed in the view. In the URLs field, type one or more URLs by which the computer can be reached. Although you can save the computer record without an Ethernet ID, the Ethernet ID is required if you want to use the network view as a client.

6 Alternatively, if the computer that you want to add has file sharing enabled, click the Browse (...) button to browse for it. Select the computer from the list and click Connect. This adds the computer as a client of the network view. If the computer does not have a computer record in the directory domain using its computer name, the directory domain adds a new record for the computer.

The server initiates a URL-based search, which looks for services with the standard file service types (AFP, SMB/CIFS, FTP, and NFS). You are able to browse through all the computers you would normally see under /Network. Select a computer from the list.

7 Click Save.

Removing Client Computers from Network Views

You can remove client computers from a network view by removing them from the client's list in the Settings pane. This list does not include all clients of the view. If you specify a network view when you create or edit a computer record, the computer isn't added to the client list in the Settings pane. To stop these computers from using this view, you must edit their computer records and specify different network views or no network view.

To remove computers from the network view's client list:

1 Open Workgroup Manager, and click Network.

2 Click the globe to choose the directory domain in which the view resides.

3 Click the lock to authenticate as a domain administrator for the directory domain.

4 In the Network Views list, select the view and click Settings.

5 Select a client in the clients list and click Delete (–).

6 Click Save.

Disabling Network View Visibility for Specific Computers

If you no longer want a computer to use a particular network view, you can do one of the following:

- Disable the view. For instructions, see "Enabling or Disabling a Network View" on page 211.
- Delete the view. For instructions, see "Deleting a Network View" on page 211.
- Disassociate the view from the related computer record. For instructions, see "Removing Client Computers from Network Views" on page 218.
- Change the view associated with the computer record. For instructions, see "Editing Computers in Network Views" on page 214.

If you've named a network view using a subnet mask in Classless Inter Domain Routing (CIDR) notation and want to avoid showing the view on any particular computer in the subnet, assign a different named view to the computer record for the computer. The view you assign can be Default, Public, or a view named using an Ethernet or IP address.

Setting the Network View Update Rate

You can set how frequently clients check for network view changes. Client computers also check for network view changes whenever they connect or disconnect to the directory server.

To set the view refresh rate:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view and click Settings.
5. In the "Clients check for changes" field, specify the number of minutes, hours, or days to wait before checking for changes. Choose minutes, hours, or days in the adjacent pop-up menu.
6. Click Save.

Setting Finder Behavior with Network Views

You can display a network view in a client computer's Finder that replaces or adds to the network resources the Finder lists.

Although you can add your network view to the Finder's network resources list, you cannot use this method to add more than one network view on the client computer. For example, if you make views named after both a client computer's Ethernet address and IP address, the client computer only displays the Ethernet address. For more information, see "How a Computer Finds Its Network Views" on page 216.

To set Finder network view display behavior:

1. Open Workgroup Manager, and click Network.
2. Click the globe to choose the directory domain in which the view resides.
3. Click the lock to authenticate as a domain administrator for the directory domain.
4. In the Network Views list, select the view and click Settings.
5. In the Settings pane, select "add to Network view" to combine the network view with the Finder's default display of network resources. Select "replace Network view" to show only the network view in the Finder.
6. Click Save.

Solving Problems

12

If you encounter problems as you work with Workgroup Manager, you may find a solution in this chapter.

If the answer to your question isn't here, try searching Mac OS X Server onscreen help for new topics. You can also search the Apple Service & Support website for information and solutions at www.apple.com/support/.

Diagnosing Common Network Issues

Before you try the individual solutions in this chapter, ensure that your network is properly configured. In particular, test your Network Time Protocol (NTP), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) services.

For more information about NTP, DNS, or DHCP, see the network services administration guide.

Testing Your Network's Time and Time Zones

The many technologies and services within Mac OS X Server rely on having accurate time settings on all of your networked computers. Typically, computers will be connected to an NTP server that provides accurate time settings to your computers. You should still check your networked computers' time settings by using Apple Remote Desktop (not included with Mac OS X Server).

You can send the following commands by using the `ssh` command. You can also test and correct a computer's time settings in System Preferences. Both of these methods allow you to test and correct only one computer at a time, whereas by using Apple Remote Desktop, you can test and correct many computers simultaneously.

To test your network computer's time and time zones:

1. In Apple Remote Desktop, send the following UNIX command to all of your computers:

```
sudo systemsetup -gettimezone
```

All of your computers should be on the same time zone. If they are not on the same time zone, send the following UNIX command:

```
sudo systemsetup -settimezone 'US/Pacific'
```

For other time zones, see the man page for `systemsetup`. For instructions on sending UNIX commands through Apple Remote Desktop, see the Apple Remote Desktop administration guide.

2 In Apple Remote Desktop, send the following UNIX command to all of your computers:

```
sudo systemsetup -gettime
```

All of your computers should have times within a few minutes of each other. If they have a wide range of times, send the following UNIX command:

```
sudo systemsetup -settime current_time
```

Replace *current_time* with the current time in military format, using HH:MM:SS (hour, minute, second) notation.

Testing Your DNS Service

Your DNS service should allow you to discover a server's domain name if given an IP address, or retrieve an IP address if given a domain name. If your computers cannot do either or these tasks, you should perform further analysis of your DNS service. For a detailed description of DNS and for instructions on configuring DNS, see the network services administration guide.

If you have Apple Remote Desktop installed, you can quickly test your entire network. In Apple Remote Desktop, create a scanner that displays computers with IP addresses within the range distributed by your DHCP server. If a computer is switched on, is not in sleep mode, and is connected to your network, the computer should be in this list. This list displays the IP address given to the computer, and the computer's host name. Computers that are not assigned host names by the DNS service are listed without host names. If a computer is listed and has an appropriate IP address and host name, the computer is receiving DHCP and DNS service. For more information about how to use scanners in Apple Remote Desktop, see the Apple Remote Desktop administration guide.

If you do not have Apple Remote Desktop installed, you can perform the following task to test a single computer's ability to receive DNS service.

To test your network's DNS service:

1 Open Network Utility on a computer in your network that is not the server that provides DNS service.

2 In the Lookup pane of Network Utility, enter the domain name of your Open Directory master server and click Lookup.

The resulting log should have an "answer" section, in which it displays the IP address of your Open Directory master server. If there is no "answer" section, or if the IP address is incorrect, perform further analysis of your DNS service.

3 In the Lookup pane of Network Utility, enter the IP address of your Open Directory master server and click Lookup.

The resulting log should have an "answer" section, in which it displays the domain name of your Open Directory master server. If there is no "answer" section, or if the domain name is incorrect, perform further analysis of your DNS service.

Note: Instead of using Network Utility, you can use the `dig` tool in Terminal. Enter the following command in Terminal:

```
dig name_or_address
```

Replace *`name_or_address`* with the domain name or the IP address of your Open Directory master server. The resulting log should have an "answer" section with either the correct IP address or domain name.

Testing Your DHCP Service

Your DHCP service should be configured to supply enough IP addresses to serve your entire network. If a computer does not have a valid IP address, it cannot be contacted through your network. For a detailed description of DHCP and for instructions on configuring DHCP, see the network services administration guide.

If you have Apple Remote Desktop installed, you can quickly test your entire network. In Apple Remote Desktop, create a scanner that displays computers with IP addresses within the range distributed by your DHCP server. If a computer is switched on, is not in sleep mode, and is connected to your network, the computer should be in this list. This list displays the IP address given to the computer, and the computer's host name. Computers that are not assigned host names by the DNS service are listed without host names. If a computer is listed and has an appropriate IP address and host name, the computer is receiving DHCP and DNS service. For more information about how to use scanners in Apple Remote Desktop, see the Apple Remote Desktop administration guide.

If you do not have Apple Remote Desktop installed, you can perform the following task to test a single computer's ability to receive DHCP service.

To test your network's DHCP service:

1 In Server Admin, click the disclosure triangle to the left of the server providing DHCP service. This displays all of the server's services.

2 Select DHCP, and click Settings.

In the Subnets pane, there is a list of the addresses that your DHCP server supplies.

3 Open Network Utility on a client computer.

If the displayed IP address is not within your range of supplied addresses, the computer is not receiving an IP address through your DHCP service.

If the IP address is 169.254.x.x, it is a self-assigned IP address. This means that your computer is receiving no DHCP service. If the IP address is not an assigned address and not 169.254.x.x, the computer is receiving DHCP service from a different DHCP server than yours.

Solving Account 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:

- The directory domain must be the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. Only these domains can be updated using Workgroup Manager.
- You must have authenticated as an administrator of the directory domain. To authenticate, click the lock (near the top of the Workgroup Manager window).

Users Can't See Their Names in the Login Window

When you upgrade to Mac OS X version 10.4 and migrate existing users to a shared directory on the new server, certain users might not show up in the login window. The login window does not list system users (users with user IDs below 500), but they can still log in by entering a user name and password.

The login window lists network users only if managed preferences are set, as described in "Specifying How a User Logs In" on page 175.

You Can't Unlock an LDAP Directory

To make changes in any directory domain, you must authenticate with the name and password of an administrator of that directory. Thus, to edit an entry in a shared LDAPv3 directory, you must authenticate in Workgroup Manager with the name and password of an administrator account in that LDAPv3 directory. (An administrator account in /NetInfo/DefaultLocalNode, which is the computer's local directory, can't be used to authenticate as an administrator of a shared LDAP directory.)

You Can't Modify a User's Open Directory Password

To modify the password of a user whose password type is Open Directory, you must be an administrator of the directory domain in which the user's record resides. In addition, your user account must have a password type of Open Directory. The user account specified when the Open Directory master was set up (using Server Assistant or the Open Directory service settings in Server Admin) has an Open Directory password. This account can be used to set up other user accounts as directory domain administrators with Open Directory passwords.

You Can't Change a User's Password Type to Open Directory

To change a user's password type to Open Directory authentication, you must be an administrator of the directory domain in which the user's record resides. In addition, your user account must be configured for Open Directory authentication. The user account specified when the Open Directory master was set up (using Server Assistant or the Open Directory service settings in Server Admin) has an Open Directory password. This account can be used to set up other user accounts as directory domain administrators with Open Directory passwords.

You Can't Assign Server Administrator Privileges

In order to assign server administrator privileges to a user for a particular server, first connect to that server in Workgroup Manager and authenticate in the directory domain. Select the user's account (or create a new account for the user), and select "User can administer the server" in the Basic pane.

Users Can't Log In or Authenticate

If a user can't log in or authenticate to their account, a number of approaches may be required to determine whether the source of the authentication problem is configuration-related or due to the password itself. Try these techniques:

- Reset the password to a known value, and then determine whether there is still a problem. Try using a 7-bit ASCII password, which is supported by most clients.
- Make sure that the password contains characters supported by the authentication protocol. Leading, embedded, and trailing spaces as well as special characters (for example, pressing Option-8 to form a bullet) are not supported by some protocols. For example, leading spaces work over POP and AFP, but not over IMAP.
- Make sure that the user's current keyboard can generate all the characters in the user's password.
- Crypt passwords don't support many authentication methods. To increase the possibility that a user's client applications are supported, set the user's password type to Open Directory or suggest that the user try a different application.
- If the user's account resides in a directory domain that is not available, create a user account in a directory domain that is available.

  For more information, see "Users Can't Log In with Accounts in a Shared Directory Domain" on page 226.
- Make sure the client software encodes the password so that it is recognized correctly. For example, Open Directory recognizes UTF-8 encoded strings, which may not be sent by some clients.
- Make sure that the user's current application and operating system support the user's password length. For example, Windows applications that use the LAN Manager authentication method support only 14-character passwords, so a password longer than 14 characters would cause an authentication failure even though Mac OS X Server's Windows service supports longer passwords.

- If you disabled any authentication methods for Open Directory passwords or shadow passwords, such as APOP or Lan Manager, and then the user's applications are unable to authenticate with the disabled methods. The Open Directory administration guide explains how to disable and enable authentication methods. After enabling or disabling Open Directory Password Server or shadow password authentication methods, you may need to reset the user's password.
- For Kerberos troubleshooting tips, see "Users Can't Authenticate Using Single Sign-On or Kerberos" on page 227.
- If a Mac OS version 8.1–8.6 computer fails to authenticate for Apple file service, the computer's AppleShare Client software may need upgrading.
  - Mac OS version 8.6 computers should use AppleShare Client version 3.8.8.
  - Mac OS version 8.1–8.5 clients should use AppleShare Client version 3.8.6.
  - Mac OS version 8.1–8.6 client computers that have file server volumes mount automatically during startup should use AppleShare Client version 3.8.3 with the DHX UAM (User Authentication Module) installed. The DHX UAM is included with the AppleShare Client version 3.8.3 installation software.

Users Relying on a Password Server Can't Log In

If your network has a server with Mac OS X Server version 10.2, it could be configured to get authentication from an Open Directory Password Server hosted by another server. If the Password Server's computer becomes disconnected from your network—for example, because you unplug the cable from the computer's Ethernet port—users whose passwords are validated using the Password Server can't log in because its IP address isn't accessible.

Users can log in to Mac OS X Server if you reconnect the Password Server's computer to the network. Alternatively, while the Password Server's computer is offline, users can log in with user accounts whose password type is crypt password or shadow password.

Users Can't Log In with Accounts in a Shared Directory Domain

Users can't log in using accounts in a shared directory domain if the server hosting the directory isn't accessible. A server may become inaccessible due to a problem with the network, the server software, or the server hardware. Problems with the server hardware or software affect users trying to log in to Mac OS X computers and users trying to log in to the Windows domain of a Mac OS X Server primary domain controller (PDC). Network problems may affect some users but not others, depending on where the network problem is.

Users with mobile user accounts can still log in to the Mac OS X computers they used previously. And users affected by these problems can log in by using a local user account defined on the computer, such as the user account created during initial setup after installing Mac OS X.

Users Can't Access Their Home Folders

Make sure that users have access to the share point in which their home folders are located, and to their home folders. Users need Read access to the share point and Read & Write access to their home folders.

Users Can't Change Their Passwords

Users who have accounts in the server's LDAP directory with a password type of "crypt password" cannot change their passwords after logging in from a client computer with Mac OS X version 10.3. These users can change their passwords if you use Workgroup Manager's Advanced pane to change their accounts' User Password Type setting to Open Directory. When you make this change, you must also enter a new password. Then you should instruct users to log in using this new password and change it in the Accounts pane of System Preferences.

Users Can't Authenticate Using Single Sign-On or Kerberos

There are several ways to remedy Kerberos authentication failures. You can find these solutions, as well as a full description of how to reconfigure a server's computer record for single sign-on and Kerberos authentication, in the Open Directory administration guide.

Solving Preference Management Problems

This section describes some problems you may encounter while using Workgroup Manager to set up accounts or manage Mac OS X clients. It also provides troubleshooting tips and possible solutions. If your problem is not addressed here, you may want to check Workgroup Manager help or consult the Apple Service & Support website (www.apple.com/support/).

You Can't Enforce Default Web Settings

If you manage Internet preferences using Workgroup Manager and set up a default web browser, a default home page or search page, or a specific location to store downloaded files, some applications may not accept these settings. You may need to set a default home page using the application's own preference settings instead.

You Can't Enforce Default Mail Settings

If you manage Internet preferences using Workgroup Manager and set up a default email reader, email address, or mail servers, some applications may not accept these settings. You may need to use the preference settings of the client computer's email application instead.

Users Don't See a List of Workgroups at Login

If a user with a network account doesn't see a list of workgroups at login:

- The user may not be in a group or may be in only one group. Hold down the Option key during login to show the list of workgroups.
- The user's computer may not be in a computer list. Add the computer to a computer list or else it will be included in the Guest Computers list.

If a user with a local account doesn't see a list of workgroups at login, add the user's computer to a computer list with multiple workgroups. Select "Local-only accounts pick workgroups from the above list." Your client computers must use Mac OS X version 10.4 or later to be able to select from these workgroups. For more information about how to set access settings for computer lists, see "Using Local User Accounts" on page 98.

Users Can't Open Files

Ordinarily, when users double-click a file in the Finder or choose a file to open from the Finder's File menu, an appropriate default application opens the file for them. If the user works in a managed environment, this method may not always work.

For example, suppose the default application for viewing PDF files is Preview. A user logs in and double-clicks a PDF file on his or her desktop. If the management settings that apply to that user don't provide access to Preview, the file does not open. If the user has access to a different application that can handle PDF files, the user can open that application and then open the file.

To make sure commonly used applications are available to users, groups, or lists of computers, use Workgroup Manager to add the application to the list of permitted applications in the Applications pane of Preferences.

Users Can't Add Printers to a Printer List

Users are able to add printers to the list of printers in Printer Setup Utility if you select Always as the management setting for Printer preferences and select "Allow user to modify the printer list." However, when a user tries to print a document from an application, any printer the user added doesn't appear in the list of available printers.

In Workgroup Manager, an administrator can make available or unavailable any number of printers to specific users, groups, or lists of computers using the Printer List pane of Printer preferences.

Note: If "Allow user to modify the printer list" is not selected, an administrator password is required to add or remove printers in Printer Setup Utility.

Login Items Added by a User Don't Open

In Workgroup Manager, you can use Login Items settings to specify items that open automatically when a user logs in. The set of items that open at login is a combination of items specified for the user, the computer being used, and the group chosen at login.

If you select Always, a user can add additional login items if you select "User may add and remove additional items." Selecting Always removes any existing items from the user's login items list and replace them with the items you list. It also prevents the user from disabling the items you list.

If you select Once, you can select "Merge with user's items," which causes one of two effects depending on whether the user already has items in their login list:

- If the user already has items listed in their login list, either from the user adding them or from having items previously added through preference management, merging only opens login items that appear on both the user's list and your list.
- If the user's login list does not include any items, all managed login items open. If you do not select "Merge with user's items," all login items on either list open. If you select Once, a user can remove any items added to their login list.

For detailed instructions on managing automatically opened items, see "Opening Items Automatically After a User Logs In" on page 176.

Items Placed in the Dock by a User Are Missing

In Workgroup Manager, you can use Dock Items settings to specify items that appear in a user's Dock. The set of items in a user's Dock is a combination of items specified for the user, the computer being used, and the group chosen at login.

If you deselect "Merge with user's Dock," all Dock items you place will override users' Dock items settings. Users cannot add additional items to their Docks if you select Always and deselect "Merge with user's Dock." Users cannot remove items from their Docks if you select Always.

For more information about how to add Dock items, see "Adding Items to a User's Dock" on page 158.

A User's Dock Has Duplicate Items

When you use Workgroup Manager to set up the same Dock item preferences for more than one kind of account (user, group, or computer), a managed user's Dock may contain duplicate items. For example, an application icon may appear more than once in the user's Dock.

This behavior does not affect any Dock items; all of them work as expected when selected. You may be able to correct this behavior by removing Dock item settings from all affected accounts, and then respecifying them.

Users See a Question Mark in the Dock

You can use Workgroup Manager to control what items a user sees in his or her Dock. Items in the Dock are actually aliases to original items stored elsewhere, such as on the computer's hard disk or on a remote server.

If you add items to a user's Dock that are only located on the server and not the user's hard disk or other volume mounted on the user's computer, the items appear as question mark icons. Clicking these icons does not open the items. If you add an item that is located on both the server and the user's computer, clicking the icon opens the item located on the user's computer or a mounted volume.

Users See a Message About an Unexpected Error

When you manage Classic preferences and try to use the Extensions Manager, File Sharing, or Software Update control panels, you may see a message that says "The operation could not be completed. An unexpected error occurred (error code 1016)." This message indicates that an administrator has restricted access to the item the user attempted to use, such as an application the user is not allowed to open.

Users are not allowed to access the control panels mentioned above when Classic preferences are managed. Users may also see the message if you have selected "Hide Chooser and Network Browser" and they attempt to use the Chooser.

The message also appears when a user tries to open an unapproved application (one that is not listed in the Items pane of the Applications preference in Workgroup Manager) in either the Classic environment or Mac OS X.

Importing and Exporting Account Information

You can use Workgroup Manager to import and export accounts and the `dsimport` command-line tool to import accounts.

You can quickly import or export user, group, and computer list accounts by using Workgroup Manager. You can also use the `dsimport` command-line tool to import user and group accounts.

Understanding What You Can Import and Export

You can import all record types that are tracked in Workgroup Manager. Some of the most prominent record types include users, groups, and computer lists. Starting with Mac OS X Server version 10.4, you can even import partial attributes of individual records. You can also combine attributes from different records. When importing from custom files, the only attribute that a record must have is a record name. For a list of attributes, open Terminal and enter `man DirectoryServiceAttributes`. Alternatively, if you have Xcode installed, you can view a list of attributes with improved formatting and more detailed descriptions by opening: /System/Library/Frameworks/DirectoryService.framework/Headers/DirServicesConst.h

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. However, you can add users to the wheel and admin groups.

You can use the `dsimport` tool to import any number of records from a text-delimited file.

See the Open Directory administration guide for descriptions of common record types and attributes. For a more complete list of attributes, enter `man DirectoryServiceAttributes`, or view the DirServicesConst.h file.

Limitations for Importing and Exporting Passwords

When creating new records or when overwriting existing records, you need to reset passwords for user accounts with Open Directory passwords or shadow passwords. Importing passwords generally works only if the password is a plain text string in the import file. Additionally, you need to set the AuthMethod attribute so that Workgroup Manager can import the password. Encrypted passwords that are in hash format in the import file cannot be recovered.

Passwords cannot be exported using Workgroup Manager or any other method. If you are importing user accounts from an export file, remember to manually set passwords or set default passwords to a known value. Before exporting user accounts (or after importing them), you can set up a password policy that requires that users change their password at first login. For instructions on configuring password options, see "Choosing a Password Type and Setting Password Options" on page 64.

Archiving the Open Directory Master

Instead of exporting and importing records as a backup of directory data, you can archive and restore the Open Directory master's directory and authentication data. By archiving a copy of the Open Directory master's directory, you can later restore the entire directory with passwords intact.

For more information and instructions on archiving the Open Directory master, see the Open Directory administration guide.

Using Workgroup Manager to Import Users and Groups

You can use Workgroup Manager to import user and group accounts into the LDAP directory of an Open Directory master or a NetInfo domain. When a file is imported, Workgroup Manager identifies the record format automatically.

Before trying to import accounts using Workgroup Manager, you should create a character-delimited or XML file containing the accounts to import, and place it in a location accessible from the computer on which you use Workgroup Manager. The LDAP directory of an Open Directory master supports files with up to 200,000 records, while local NetInfo databases support files with up to 10,000 records.

Important: Workgroup Manager can only import files that use UNIX line breaks. When editing import files, use a text editor that supports UNIX line breaks.

For information about how to create files to import, see the following topics:

- "Using XML Files Created with Mac OS X Server Version 10.1 or Earlier" on page 234
- "Using XML Files Created with AppleShare IP 6.3" on page 235
- "Using Character-Delimited Files" on page 236

To import accounts using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.

   See the Open Directory administration guide for instructions.
3. Click the globe, and then choose the domain in which you want to import accounts.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Choose Server > Import, and select an import file.
6. 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 multivalue attribute in the existing account. Duplicates are not created. This option might be used, for example, when importing new members into an existing group.

   "Don't check for duplicates" disables checking for duplicates, but it can cause misconfigured records and unexpected results. You should first ensure that there are no duplicates before choosing this option. When you enable this, it can decrease the time required to import.
7. To enable presets for a user or a group, select Preset for Users or Preset for Groups and choose a preset from the two lists. For more information about how to create presets, see "Creating a Preset for User Accounts" on page 55 and "Creating a Preset for Group Accounts" on page 80.
8. In the First User ID field, you can enter the user ID at which to begin assigning user IDs to new user accounts for which the import file contains no user ID.
9. In the Primary Group ID field, you can enter the group ID to assign to new user accounts for which the import file contains no primary group ID.
10. Click Import.

Using Workgroup Manager to Export Users and Groups

You can use Workgroup Manager to export user and group accounts from the LDAP directory of an Open Directory master or a NetInfo domain into a character-delimited file that you can import into a different NetInfo or LDAP domain.

To export accounts using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server you're using have been configured to access the desired directory domain.

   See the Open Directory administration guide for instructions.
3. Click the globe, and then choose the domain in which you want to import accounts.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Users button to export users, or the Groups button to export groups.
6. To export a specific account, click the account. To export all accounts listed, select all of them. To choose multiple accounts to export, select the accounts while holding the Command or Shift key.
7. Choose Server > Export.
8. Specify the name to assign to the export file and the location where you want to create it.
9. Click Export.

Using dsimport to Import Users and Groups

You can use the `dsimport` command-line tool to import user and group accounts into a directory. `dsimport` permits logging at three levels with the `-l` switch.

You can use the `dsimport` tool to import any number of records from a text-delimited file. For more information about these attributes, open Terminal and type `man DirectoryServicesAttributes`.

See the Open Directory administration guide for a list of record types, their standard attributes, and the accepted values of the attributes.

In order to use `dsimport` or to view `DirectoryServicesAttributes`, you may have to use the ssh tool to connect to the Mac OS X Server computer. For instructions on using `dsimport`, type `man dsimport` in Terminal. Alternatively, you can find detailed instructions in the command-line administration guide.

Using XML Files Created with Mac OS X Server Version 10.1 or Earlier

You can use Server Admin in Mac OS X Server version 10.1 or earlier to create an export file, and import that file into the LDAP directory of an Open Directory master or a NetInfo domain using Workgroup Manager or `dsimport`.

The following user account attributes are exported into these XML files. An error occurs when you import a file with missing required attributes.

- indication of whether user can log in
- indication of whether user is a server administrator
- user ID (required)
- primary group ID (required)
- shell
- comment
- short name (required)
- long name (required)
- password format (required) and password text (required)
- Apple mail data
- ara (Apple Remote Access; this data is ignored)

The following group account attributes might be present in these XML files. If there are group accounts present, then the required group attributes must be included.

- group name (required)
- group ID (required)
- one member's short name (required)
- other members' short names

Using XML Files Created with AppleShare IP 6.3

You can use the Web & File Admin application on an AppleShare IP 6.3 server to create an export file, and then use Workgroup Manager or `dsimport` to import that file into the LDAP directory of an Open Directory master or a NetInfo domain.

The following user account attributes are exported into these XML files. An error occurs when you import a file with missing required attributes.

- name (required, mapped to a long name)
- inetAlias (mapped to a short name)
- comment
- indication of whether user can log in
- password format (required) and password text (required)
- 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 `dsimport` tool generates user IDs when you import this XML file, using the `-s` parameter to determine the user ID to start with and incrementing each subsequently imported account's user ID by one. It generates primary group IDs using the `-r` parameter. When you import using Workgroup Manager, user IDs and primary group IDs are generated as you indicate in the dialog provided.

The following group account attributes might be present in these XML files:

- group name (required)
- one member's short name (required)
- other members' short names

The `dsimport` tool 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.

Using Character-Delimited Files

You can export a character-delimited file by using Workgroup Manager to export accounts in the LDAP directory of an Open Directory master or a NetInfo domain. You can also create a character-delimited file by hand or by using a database or spreadsheet application.

The first entry in the file is a record description that characterizes the format of each of the accounts listed in the file. The entries in the file describe user or group accounts, encoded in the format described by the first entry.

Writing a Record Description

A record description identifies the fields in each record you want to import from a character-delimited file. It indicates how records, fields, and values are separated. It also describes the escape character that precedes special characters in a record.

You can use Workgroup Manager to import accounts without record descriptions. When you import an account without a record description, Workgroup Manager displays a dialog that allows you to map attributes found in the imported file. If the imported file has a record description, you do not see this dialog.

To write the record description, use the following elements in the order specified, separating them with 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 have a record name and should include the following in order to be complete:

- RecordName (the user's short name)
- RealName (the user's long name)
- NFSHomeDirectory
- Password
- UniqueID (the user ID)
- PrimaryGroupID

You can omit UniqueID if you specify a first user ID when importing. You can omit PrimaryGroupID if you specify a default primary group ID when importing.

In addition, you can include:

- UserShell (the default shell)
- NFSHomeDirectory (the path to the user's home folder on the user's computer)
- Other user data types described in the Open Directory administration guide

For group accounts, the list of attributes must include:

- RecordName (the group name)
- PrimaryGroupID (the group ID)
- GroupMembership

The following is an example of a record description:

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Users 7
RecordName Password UniqueID PrimaryGroupID
RealName NFSHomeDirectory UserShell
```

In this example, attribute names don't include the optional prefix `dsAttrTypeStandard:`. You can include this prefix or omit it in your own character-delimited import files. If you use Workgroup Manager to export a character-delimited file, it includes this prefix with each attribute name. Here is an example of a record encoded using the description:

```
jim:Ad147E$:408:20:J. Smith, Jr., M.D.:/Network/Servers/somemac/Homes/jim:/
     bin/csh
```

The record consists of values, which are delimited by colons. Use a double colon (::) to indicate a missing value.

When importing user passwords, you can insert the following in the list of attributes to set the user's password type to Open Directory:

```
dsAttrTypeStandard:AuthMethod
```

The method for setting an imported user's password type to Open Directory requires that the imported data actually have a password value. If the password value is missing for a user, then the corresponding user record is created with a password type of crypt or shadow password.

Then insert the following in the formatted record (in this example, the user 's password is "pw"):

```
dsAuthMethodStandard\:dsAuthClearText:pw
```

Note: In this example, the colon (:) is the field separator. Because there is a colon in the description for this attribute, the escape character must be used to indicate that the colon should not be treated as a delimiter. The backslash (\ ) is the escape character in this example. If the field separator is anything other than the colon, the escape character is not needed.

This is an example of a header from a standard users import file with users who have Open Directory passwords. Although presented here on multiple lines, in an import file it must be one line of text in which the elements are separated by spaces and without line breaks.

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Users 8
dsAttrTypeStandard:RecordName dsAttrTypeStandard:AuthMethod
dsAttrTypeStandard:Password dsAttrTypeStandard:UniqueID
dsAttrTypeStandard:PrimaryGroupID dsAttrTypeStandard:Comment
dsAttrTypeStandard:RealName dsAttrTypeStandard:UserShell
```

This is an example of a formatted record with the following attributes and values:

```
<Attribute>: <Value>
Record Name (short name): tuser
Authentication Method: dsAuthClearText
Password: pw
Unique ID: 1242
Primary Group ID: 20
Comment: <blank>
Real Name (long name): Terri User
User Shell: /bin/tcsh
tuser:dsAuthMethodStandard\:dsAuthClearText:pw:1242:20::Tom User:/bin/tcsh
```

Note: This example also uses the colon (:) as the field separator and the backslash (\) as the escape character.

ACL Permissions and Group Memberships Using GUIDs

Mac OS X Server version 10.4 introduces a new user and group attribute for determining file system permissions and group membership.

Mac OS X version 10.4 departs from the historical UNIX practices of:

- Basing file system permissions only on the user ID (UID) and group ID (GID) attributes
- Basing group membership on the user short name

By introducing globally unique identifiers (GUIDs), Mac OS X version 10.4 can now augment standard POSIX file system permissions with access control lists (ACLs). GUIDs also enable nested group membership in Mac OS X version 10.4.

GUIDs do not remove or change POSIX permissions, nor do they affect interoperability of Mac OS X with legacy UNIX systems or other operating systems.

Understanding GUIDs

Beginning with Mac OS X version 10.4, a universal ID called a globally unique identifier (GUID, pronounced GOO-id) provides user and group identity for ACL file system permissions. The GUID also provides membership for a user to groups and nested groups.

The administration tools in Mac OS X Server version 10.2 and later automatically assign a new GUID to every new user account and to every user account that's imported, but Mac OS X version 10.4 is the first version to use GUIDs and to include GUIDs in export files.

Two users can have identical long names, short names, UIDs, and GIDs, but they have different GUIDs. Thus they can have different ACL permissions and can belong to different groups. Since their GUIDs are 128-bit values, it is extremely unlikely to have duplicate GUIDs.

As an administrator, you must now make sure you can restore user accounts with GUIDs intact. Restoring user accounts with UID, GID, and short name but no GUID does not restore ACL permissions or group membership in Mac OS X version 10.4 or later. For more information about how to maintain and restore GUIDs, see "Maintaining GUIDs When Importing from Earlier Versions of Mac OS X Server" on page 242.

Mac OS X version 10.4 verifies group and nested group membership by checking GUIDs. A group's GUID is also used by file system ACLs and is stored on disk in the access control entry (ACE). Legacy user short names are used only if there are no GUIDs present in the group record.

GUIDs and File Permissions

ACLs use GUIDs to determine file ownership and access permissions, while POSIX uses UIDs to determine file ownership and permissions.

ACLs and POSIX Permissions

An ACL is a list of access control entries (ACEs), each specifying permissions to be granted or denied to a user or group for accessing a folder and its contents. Users and groups are identified in ACLs by their GUIDs. An ACL also specifies how its permissions propagate through a folder hierarchy. You can set ACL permissions in addition to standard POSIX permissions.

Every file and folder always has POSIX permissions. Unless an administrator assigns ACL permissions, the POSIX permissions continue to determine user access in a Mac OS X version 10.4 system. If you assign ACL permissions, they take precedence over the standard POSIX permissions.

If a file has ACL permissions but none apply to the user, the POSIX permissions will determine user access. If a file has multiple ACEs that apply to a user, the first applicable ACE listed takes precedence and the following ACEs are ignored.

For more information about ACL and POSIX permissions, see the file services administration guide.

File Permissions and Synchronization

Having the same POSIX permissions for files synchronized between two computers requires having the same UID on both computers. Having the same ACL permissions on both computers requires matching GUIDs as well. This can be done using Workgroup Manager or command-line directory editing tools, or simply by having both computers share the same directory domain.

Portable Home Directories (PHDs) rely on a user having the same GUID in the local user account on the user's computer and in the network user account on an Open Directory server. This ensures that file permissions are the same whether the user logs in using the local user account (while disconnected from the network) or the network user account.

SIDs and Windows Interoperability

Security identifiers (SIDs) for Windows systems have similar functions to GUIDs on Mac OS X systems. Every time Mac OS X assigns a GUID to a process or a file, a SID is assigned as well. When servers and clients interact using the SMB protocol, they transfer SIDs and not GUIDs. When Mac OS X Server receives SIDs, it automatically retrieves the user accounts with the corresponding GUIDs.

If a user account moves to a different Active Directory domain, it gets a new SID but not a new GUID. The user still has the access permissions assigned to old SIDs, because Active Directory keeps track of SID history in user accounts. This allows Mac OS X systems to work seamlessly with Windows systems.

GUIDs and Group Memberships

Mac OS X Server version 10.4 uses GUIDs and a combination of the user's short name and GID to determine group membership. Previously, group membership was based only on a combination of the user's short name and GID.

You can have groups composed of users with earlier versions of Mac OS X and Mac OS X version 10.4 installed. When you use Workgroup Manager on Mac OS X Server version 10.4 to add a member to a group, you add both the user's short name and GUID. Adding both attributes ensures backward-compatibility.

Importing and Exporting GUIDs

When importing accounts, make sure to use files exported from Workgroup Manager on Mac OS X Server version 10.4. This ensures that accounts keep their GUIDs intact.

Consider replacing all of your existing account backup files with updated backup files to ensure that the GUIDs transfer correctly.

Maintaining GUIDs When Importing from Earlier Versions of Mac OS X Server

GUIDs (globally unique identifiers) are used in Mac OS X Server version 10.4 to verify user and group identity for ACL permissions and to manage user membership in groups and nested groups. When you use Workgroup Manager or the `dsimport` tool to import users and groups created on versions of Mac OS X Server earlier than 10.4, GUIDs are automatically assigned.

After upgrading or migrating your server to Mac OS X Server version 10.4, you should back up your accounts by exporting existing user and group accounts, which now have GUIDs. If you need to restore user or group accounts in the future, this new export file enables you to import the users and groups with their GUIDs intact.

To make sure that GUIDs and their relationship to specific users and groups remain the same if you need to reimport the same users and groups, create a new export file on Mac OS X Server version 10.4 and use this file instead of the export file created using an earlier server version.

Using GUIDs When Importing and Exporting Users

Having an export file that contains a GUID for every user and group enables you to quickly restore users and groups with file permissions and group memberships unchanged. The GUID attribute is automatically included when you export user records from Workgroup Manager or the command line in Mac OS X Server version 10.4.

If you lose user accounts and create new accounts with the same UID, GID, and short names as the lost accounts, the replacement accounts have new GUIDs assigned. A user's new GUID won't match the previous GUID, so the user won't retain prior ACL permissions or group memberships. Similarly, If you import users or groups from a file that doesn't include the GUID attribute, Mac OS X Server assigns new GUIDs to every imported user and group.

Working with GUIDs

Although you can view and modify most user account attributes using the Accounts pane in Workgroup Manager, you need to use the Inspector to view and modify GUIDs.

Viewing GUIDs

GUIDs are stored in the directory domain and are not immediately visible in Workgroup Manager. To view GUIDs, you must first enable the Inspector in Workgroup Manager. For instructions on using the Inspector, see the Open Directory administration guide.

> ***Warning:*** Although you can use the Inspector to edit GUIDs, you should not edit GUIDs because doing so destroys existing group memberships and file permissions for that user ID.

To view a user or group GUID:

1. In Workgroup Manager, click Accounts.
2. Ensure that the directory services of the Mac OS X Server computer you're using have been configured to access the desired directory domain.
3. Click the globe, and then choose the domain in which the account resides.
4. To authenticate, click the lock and enter the name and password of a directory domain administrator.
5. Click the Users, Groups, or Computer Lists button, and select the account. You cannot view GUIDs for multiple accounts simultaneously.
6. Click the Inspector button located under the lock on the far right.

   If there is no Inspector button, make sure that the Inspector is enabled by choosing Workgroup Manager > Preferences, and then selecting "Show 'All Records' tab and Inspector."
7. Select the GeneratedUID field and then click Edit.
8. Click Cancel to ensure that you do not change the GUID.

Glossary

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

access control list See **ACL**.

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

Active Directory The directory and authentication service of Microsoft Windows 2000 Server and Windows Server 2003.

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've installed the server administration 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.

Apple Filing Protocol See **AFP**.

automount To make a share point appear automatically on a client computer. See also **mount**.

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

child A computer that gets configuration information from the shared directory domain of a parent.

computer account See **computer list**.

computer list A list of computers that have the same preference settings and are available to the same users and groups.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically 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, 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. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

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 be created only 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.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a website visitor.

export In the Network File System (NFS), a way of sharing a directory with clients on a network. TBD for RAID context.

filter A "screening" method used to control access to a 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.

full name See **long name**.

globally unique identifier See **GUID**.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group folder A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among themselves.

guest computer An unknown computer that isn't included in a computer list on your server.

guest user A user who can log in to your server without a user name or password.

GUID Globally unique identifier. A hexadecimal string that uniquely identifies a user account, group account, or computer list. Also used to provide user and group identity for access control list (ACL) permissions, and to associate particular users with group and nested group memberships. GUIDs are 128-bit values, which makes the generation of duplicate GUIDs extremely unlikely.

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 Mac OS 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 webpage's words and images for the user.

HTTP Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. The HTTP protocol provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

idle user A user who is connected to the server but hasn't used the server volume for a period of time.

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

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

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

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

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

load balancing The process of distributing client computers' requests for network services across multiple servers to optimize performance.

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

local home directory A home directory that resides on disk on the computer a user is logged in to. It's accessible only by logging directly in to the computer where it resides unless you log in to the computer using SSH.

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

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

managed client A user, group, or computer whose access privileges and/or preferences are under administrative control.

managed network The items managed clients are allowed to "see" when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a "network view."

managed preferences System or application preferences that are under administrative control. Workgroup Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients.

mount (verb) In general, to make a remote directory or volume available for access on a local system. In Xsan, to cause an Xsan volume to appear on a client's desktop, just like a local disk.

multicast DNS A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. Called "Bonjour" (previously "Rendezvous") by Apple, this proposed Internet standard protocol is sometimes referred to as "ZeroConf" or "multicast DNS." For more information, visit www.apple.com or www.zeroconf.org. To see how this protocol is used in Mac OS X Server, see **local hostname**.

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

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've installed NetBoot software and have configured to allow clients to start up from disk images on the server.

NetInfo One of the Apple protocols for accessing a directory domain.

network view See **managed network**.

NFS Network File System. A client/server protocol that uses Internet Protocol (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.

NTP Network time protocol. A network protocol used to synchronize the clocks of computers across a network to some time reference clock. NTP is used to ensure that all the computers on a network are reporting the same time.

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 Directory master A server that provides LDAP directory service, Kerberos authentication service, and Open Directory Password Server.

owner The owner of an item can set Read & Write, Read only, or No Access permissions for Owner; Group; and Others. The owner also can assign ownership of an item to another user, and Group privileges to another group. By default the owner has Read & Write permissions.

parent A computer whose shared directory domain provides configuration information to another computer.

password An alphanumeric string used to authenticate the identity of a user or to authorize access to files or services.

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

portable home directory A portable home directory provides a user with both a local and network home folder. The contents of these two home folders, as well as the user's directory and authentication information, can be automatically kept in sync.

predefined accounts User accounts that are created automatically when you install Mac OS X. Some group accounts are also predefined.

preference manifest A file that describes the structure of and default values for an application's preferences (for example, what the various preference keys do). Workgroup Manager's preferences editor uses these files to make it easier for an administrator to edit an application's managed preferences.

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 Workgroup 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.

print queue An orderly waiting area where print jobs wait until a printer is available. The print service in Mac OS X Server uses print queues on the server to facilitate management.

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

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.

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.

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.

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.

security identifier See **SID**.

share point A folder, hard disk (or hard disk partition), or CD that's 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.

SID Security Identifier. A unique value that identifies a user, group, or computer account in a Windows NT-compatible domain.

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 DA Service Location Protocol 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/CIFS Server Message Block/Common Internet File System. 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/CIFS to provide access to servers, printers, and other network resources.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

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. See also **IP subnet**.

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.

UID User ID. A number that uniquely identifies a user within a file system. Mac OS X computers use the UID to keep track of a user's directory and file ownership.

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.

user name The long name for a user, sometimes referred to as the user's "real" name. See also **short name**.

user profile The set of personal desktop and preference settings that Windows saves for a user and applies each time the user logs in.

virtual user An alternate email address (short name) for a user. Similar to an alias, but it involves creating another user account.

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.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

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.

XML An extensible markup language, similar to HTML but more formal and more flexible.

Index

A

access
- CDs and DVDs 184
- to disk and server icons 166
- to folders 169
- to group share point 177
- hard drives and disks 184
- to iDisks 168
- to media 183
- to menu items (Restart, Shut Down) 170
- network home folder 177
- POSIX and GUIDs 27
- to remote servers 168

access settings
- about 97
- allowing access 98
- restricting access 97

accounts
- *See also* user accounts, group accounts, computer lists
- batch editing 47
- finding specific 46
- mobile accounts 115
- overview 22
- refreshing the list of 45
- searching 46
- sorting 46

ACEs (access control lists) 240

ACLs (access control lists)
- about 27
- GUIDs 239
- nested groups 81
- restricting access 125

administrator accounts
- determining requirements 37
- directory domain 23, 37, 40
- local 22
- overview 22
- privileges 62
- server 22

administrator computer
- overview 30
- setting up 40

AFP (Apple Filing Protocol)
- encrypting files 126
- hosting home folders 36
- setting up share points using 105

Apple menu 154

Apple Remote Desktop 136

Applications preferences
- about 148
- denying access 149
- helper applications 149
- providing access 148
- UNIX, access to 150

authenticating 41

automatic logout 180

B

backup
- administrator accounts 48
- directory domain 48

basic settings
- defining short names 58
- defining user names 57
- overview 57

battery status 163

Burn Disc command 169

C

Classic preferences
- about 151
- access to Apple menu 154
- Classic startup 152
- consistent preferences 155
- restarting and rebuilding 153
- System Folder 152

Classic System Folder 152

client management
- about 127
- managing preferences 143

comments
- for computer lists 92
- editing 66

computer address 90

computer lists

about 89
adding computers to 94
All Computers list 90
creating 92
deleting 96
Guest Computers 90
moving computers 95
overview 25
preexisting 89, 90
preference management 146
presets 93
removing computers from 95
searching for 96
using a preset 93
for Windows computers 90
Windows Computers list 90
computers
See also computer lists
editing information about 95

D

desktop appearance 170
DHCP (Dynamic Host Configuration Protocol) 223
DNS (Domain Name System) 222
Dock preferences
about 156
adding items 158
basic control 157
controlling modification 159
group folders 157
`dsimport` tool 234

E

ejecting disks
automatic 185
prevention 168
email preferences 173
Energy Saver preferences
about 160
automatic startup 163
battery status 163
portable computers 161
sleep 160
exporting account information
about 231
AppleShare IP XML files 235
character-delimited files 236
limitations 232
Server Admin XML files 234
using GUIDs 242
with Workgroup Manager 43, 232, 233

F

Fast User Switching 179
filename extensions 167
Finder preferences
about 164
desktop appearance 170
displaying disks and servers 166
filename extensions 167
Finder window behavior 166
Finder window contents 171
folder access 169
hiding Burn Disc 169
hiding Trash alert 167
iDisk 168
preventing disk ejection 168
remote servers 168
removing Restart and Shut Down 170
Simple Finder 165
Finder windows 171
finding accounts
accounts list 43
available directory domains 45
local directory domain 44
search policy 44

G

globe 42
group accounts
about 77
adding users to 68, 83
creating 79
defining IDs for 85
deleting 82
editing 80
legacy 81
member settings 83
naming 84
nested 81
overview 24
predefined 78
preference management 145
presets 80
primary group 67
read-only 82
removing users from 68, 84
reviewing membership 69
storage 78
group folders
about 128
Dock preferences 157
in an existing share point 86
in a share point subfolder 86
making accessible to multiple groups 88
overview 25
setting up 86
specifying no group folder 86
group settings 67
guest computers

about 25
portable computers 122
working with 91
guest users 24
GUIDs (globally unique identifiers)
about 239
ACLs 240
duplicate names 59
file permissions 241
group membership 241
importing and exporting 241
maintaining when importing 242
SIDs 241
synchronization 241
using for importing and exporting 242
viewing 243

H

Hearing preferences 200
help 15
home folders
about 101
across multiple servers 103
AFP 105
creating for local users 108
custom 110
default 113
deleting 113
distribution 36
having none 107
Mac OS X clients 102
moving 113
network 109, 128
NFS 106
other clients 103
proliferation 119
setting disk quotas for 113
setting up 101
structure 35
for Windows computers 102

I

importing account information
about 231
AppleShare IP XML files 235
character-delimited files 236
dsimport tool 234
limitations 232
maintaining GUIDs 242
Server Admin XML files 234
using GUIDs 242
with Workgroup Manager 43, 232
info settings 74
Internet preferences
about 172
email 173
web browser 173

K

Keyboard preferences 201
keywords
applying 66
master list, editing 65

L

lock 42
Login preferences
about 174
automatically opening items 176
automatic logout 180
enabling scripts 181
group share point 177
login window 175
network home folder 177
password hints 179
preventing restart and shut down 178
running scripts 182
simultaneous multiple users 179
login settings 63

M

Macintosh Manager 41
mail settings
disabling service 71
enabling service 70
forwarding 71
overview 69
managed preferences
See also preference management
about 143
caching 142
interaction 139
permanence 141
Media Access preferences
about 183
automatic ejection 185
CDs and DVDs 184
hard drives and disks 184
mobile accounts
about 115
advantages 117
alternatives 122
creating 186
disadvantages 119
logging in 116
network accounts 118
portable home directories 116
preventing creation 187
removing 188
setting up 121

synchronization frequency 190
synchronizing 120
synchronizing folders 189
mobile clients
security 124
without mobile accounts 122
Mobility preferences
about 186
creating mobile accounts 186
preventing mobile account creation 187
removing mobile accounts 188
synchronization frequency 190
synchronizing folders 189
Mouse preferences 201

N

NetBoot
images 129
overview 21
starting up computers 135
Network Install
images 129
installing software 135
overview 21
Network preferences
about 191
bypassing proxy servers 192
proxy server ports 191
network traffic
reducing 118
synchronizing 121
network views
about 13, 208
adding clients 217
adding computers 212
adding dynamic lists 215
adding neighborhoods 211
computer 208
creating 209
Default view 208
deleting 211
deleting computers 214
deleting dynamic lists 215
deleting neighborhoods 212
disabling visibility 219
dynamic list 208
editing computers 214
enabling or disabling 211
Finder behavior 220
finding 216
named view 208
naming 217
neighborhood 208
Public view 208
removing clients 218
renaming 210
types 208
update rate 219
NFS (Network File System)
setting up share points using 106
UNIX servers 36
NTP (Network Time Protocol) 221

O

Open Directory
account storage 49
archiving 232
server setup 30

P

password options 61, 64
passwords
hints 179
importing and exporting 232
unable to modify 224
password type 64
PDC (Primary Domain Controller) 31
permissions
AFP 24
anonymous users 54
groups 83
portable computers
configuring 121
Energy Saver settings for 161
multiple local accounts 123
one primary local user 123
unknown 122
portable home directories
about 13, 116
synchronizing 120, 189, 190, 241
POSIX 240
preference editor
about 14, 142, 203
adding applications 204
disabling management 206
editing application preferences 204
preference management
Applications preferences 148–151
cache 143, 144
Classic preferences 151–156
computer lists 146
customizing the user experience 129
disabling 147
Dock example 130
Dock preferences 156–159
editing multiple records 147
Energy Saver preferences 160–164
Finder preferences 164–172
group accounts 145
icon indicator 143

Internet preferences 172–174
login example 131
Login preferences 174–183
Media Access preferences 183–185
Mobility preferences 186–190
Network preferences 191–192
Printing preferences 193–196
Software Update 196
System Preferences 197
Universal Access preferences 198–202
user accounts 145
workflow example 134
preference manifest 14, 203
preferences cache
about 143
updating 144
presets
about 47
computer lists 93
creating 55
deleting 56
editing 56
for group accounts 80
renaming 56
using 55
Printing preferences
about 193
access to printers 193, 194
default printer 195
preventing printer list modification 194
restricting access 195
print settings
deleting print quota 73
disabling queue access 73
enabling queue access 72
overview 72
resetting queue 73
privileges
directory domain administrator 62
server administrator 62

R

record description 236
requirements
directory services 33
server and storage 34

S

scripts
enabling 181
running 182
search policy 44
security
about 124
directory services 126
FileVault 126
preventing access 125
Seeing preferences 199
Server Admin
overview 20
setup overview 29
share points
AFP 105
local 104
NFS 106
overview 31
working with 43
SIDs (security identifiers) 241
Simple Finder 165
sleep settings 160
Software Update preferences 196
startup and shutdown settings 163
strategies
duplicate names 59
home folder distribution 36
home folder structure 35
mobile accounts 117
NetBoot and Network Install 135
planning 33
preference management 134
security 125
service allocation 34
share points 34
short names 59
synchronizing 120
System Preferences 197

T

troubleshooting 221–230
adding printers 228
administrator privileges 225
authentication 225
common network issues 221
DHCP 223
DNS 222
Dock question mark icon 230
duplicate Dock items 229
home folders 227
LDAP 224
logging in 225
login items 229
login window 224
login workgroup list 228
mail settings 227
missing Dock items 229
NTP 221
Open Directory password 224, 225
opening files 228
passwords 227
Password Server 226

shared directory domain 226
unexpected error message 230
users and groups 224
web settings 227

U

Universal Access preferences
about 198
assistive devices 202
Hearing preferences 200
Keyboard preferences 200
Mouse preferences 201
Seeing preferences 199
shortcuts 202
UNIX
controlling access to UNIX tools 150
and GUIDs 27
home folders 36
upgrading 41
user accounts
batch editing 52
comments 66
creating 51
deleting 54
disabling 54
editing 52, 53
guest users 54
keywords 66
local 98
overview 23, 49
predefined 50
preference management 145
primary group 67
read-only 53
storage 49
user IDs 60
user information
about 14
editing 74

W

web browser preferences 173
Windows computers
configuration 30
home folders 102
PDC 31
Windows Computers list 90
Workgroup Manager 75
Workgroup Manager
accessing accounts 43
batch editing 147
exporting users and groups 233
importing users and groups 232
managed preferences 138
overview 19
using 42
workgroups
See also group accounts
overview 24