Mac OS X Server
User Management

For Version 10.3.3 or Later

034-2529/02-06-04

Contents

How to Use This Guide

This guide tells you how to use Workgroup Manager and Macintosh Manager to set up and manage home directories, accounts, preferences, and settings for clients.

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, "User Management for Mobile Clients," discusses considerations for managing portable computers.
- Chapters 4, 5, 6 tell you how to use Workgroup Manager to set up users, groups, and computer lists.
- Chapter 7, "Setting Up Home Directories," covers creating home directories.
- Chapter 8, "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 9, "Managing Preferences," describes how to use Workgroup Manager to control preference settings for users, groups, and computers that use Mac OS X.
- Chapter 10, "Using Macintosh Manager for Mac OS 9," covers how to use Macintosh Manager to control privileges and settings for users, groups, and computers that use Mac OS 9.1.
- Chapter 11, "Solving Problems," helps you address issues involving account creation, home directory maintenance, preference management, or client setup and also helps you solve problems encountered by managed clients.
- Appendix, "Importing and Exporting Account Information," provides information you'll need when you want to transfer account information to or from an external file.
- The Glossary defines terms you'll encounter as you read this guide.

Getting Help for Everyday Management Tasks

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

Related Documents

This guide refers to other texts in the server administration suite of documents. Titles of documentation that may be of particular interest in relation to user management are listed in the table below. You can find most of these texts on your Mac OS X Server software CD. Alternatively, you can download the documents from the Mac OS X Server website: www.apple.com/server/documentation.

Mac OS X Server Documents	Content
Mac OS X Server Command-Line Administration For Version 10.3 or Later	How to use a command-line interface to work with Mac OS X Server
Mac OS X Server Getting Started For Version 10.3 or Later	An overview of features and services provided in Mac OS X Server
Mac OS X Server File Services Administration For Version 10.3 or Later	How to set up sharing and other file services to allow data storage, data retrieval, and collaboration
Mac OS X Server Mail Service Administration For Version 10.3 or Later	How to set up and administer mail service for users
Mac OS X Server Migration to Version 10.3 or Later	Advice for transferring data and updating clients to use Mac OS X Server and related applications, such as Macintosh Manager
Mac OS X Server Network Services Administration For Version 10.3 or Later	Information about setting up and using services such as DHCP
Mac OS X Server Open Directory Administration For Version 10.3 or Later	How to set up and maintain integrated directory services
Mac OS X Server System Image Administration For Version 10.3 or Later	How to create and distribute system images and resource packages using tools such as NetBoot and Network Install
Mac OS X Server Print Service Administration For Version 10.3 or Later	How to set up and maintain network print services
Mac OS X Server QuickTime Streaming Server Administration For Version 10.3 or Later	Information about providing access to audio and visual media in real time

Mac OS X Server Documents	Content
Mac OS X Server Web Technologies Administration For Version 10.3 or Later	How to configure, serve, and monitor web sites using Mac OS X Server
Mac OS X Server Windows Services Administration For Version 10.3 or Later	How to integrate Windows machines into your network

Where to Find More Information About User Management

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

If You're New to Server and Network Management

To learn more about Mac OS X Server, see the website: www.apple.com/macosx/server/.

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

The AppleCare support site's discussion boards are an additional source of information: www.info.apple.com/.

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

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

If You're an Experienced Server Administrator

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

- You can obtain a variety of relevant books from O'Reilly & Associates See the O'Reilly & Associates website: www.ora.com.
- For detailed information about Apache, go to: www.apache.org/.

User Management Overview

1

This chapter introduces important 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 directories, to fine-tuning the user experience by managing preferences and settings for users, groups, and computers. Mac OS X Server provides tools for accomplishing all these tasks.

Tools for User Management

Primary user management tools and applications in Mac OS X Server include Workgroup Manager, Server Admin, NetBoot, and Network Install.

Workgroup Manager

Workgroup Manager is a powerful tool that delivers a range of features for comprehensive management of Macintosh clients. You can use Workgroup Manager directly from the server, or you can install Workgroup Manager independently of the Mac OS X Server software on a non-server client computer.

Workgroup Manager provides network administrators with a centralized method of managing Mac OS X workstations, controlling access to software and removable media, and providing a consistent, personalized experience for users at different levels, whether they're beginners in a classroom or advanced users in an office. Mac OS X Server saves user documents and preferences in a home directory, so your users can access their files from any Mac on your network. Using Workgroup Manager, you can create user accounts and then set up groups to provide convenient and efficient access to resources. You can also use account settings and managed preferences to allow more or less flexibility to suit the level of administrative control you need.

When Workgroup Manager is used in conjunction with other Mac OS X Server services, you can:

- Connect users to one another, using services such as mail and file sharing.
- Share system resources, such as printers and computers, maximizing their availability as users move about and making sure that disk space and printer usage remain equitably shared.
- Host Internet services, such as websites and streaming video.
- Customize working environments, such as desktop resources and personal files, of network users.

Preference Management

You can use Mac OS X Server's Workgroup Manager application to tailor the work environments of Mac OS X clients. Preferences you define for individual users, groups of users, and computers provide your Macintosh users with a consistent desktop, application, and network appearance regardless of the Macintosh computer to which they log in. Any preferences you define for a Mac OS X user are stored in the user's account.

To manage Mac OS 9 clients, you use Macintosh Manager, described in Chapter 10, "Using Macintosh Manager for Mac OS 9." Preferences you define for Mac OS 9 users are stored using Macintosh Manager.

To learn more about client management tools and concepts, read Chapter 8, "Client Management Overview."

Home Directories

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

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

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

You can set up a mobile account so that it has a local home directory on each client as well as a network home directory. That way a user can work offline and, when connected to the network, manually synchronize documents by copying them from the client to the network home directory. For more information about mobile accounts, see Chapter 3, "User Management for Mobile Clients."

Mail Settings

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

Mail account settings let you control a user's access to mail services running on a particular Mac OS X Server. For mail accounts residing on servers using versions of Mac OS X earlier than 10.3, you can also manage account characteristics such as how to handle automatic message arrival notification.

For details on settings for Mac OS X mail service, see the mail service administration guide.

Resource Usage

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

Mail and disk quotas limit the number of megabytes available for a user's mail or files.

Print quotas limit the number of pages a user can print using Mac OS X Server print services. Print quotas also can be used to disable a user's print service access altogether. User print settings work in conjunction with print server settings, which are explained in the print service administration guide.

Server Admin

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

For more information about using Server Admin tools, refer to the documents listed in the table below.

If you want to	Read about	In this document
Assign access privileges to folders and files within a share point	File sharing	Mac OS X Server File Services Administration For Version 10.3 or Later
Share printers among users	Print service	Mac OS X Server Print Service Administration For Version 10.3 or Later
Set up websites or WebDAV support on the server	Web service	Mac OS X Server Web Technologies Administration For Version 10.3 or Later
Provide email service for users	Mail service	Mac OS X Server Mail Service Administration For Version 10.3 or Later
Broadcast multimedia in real time from the server	QuickTime Streaming Service	Mac OS X Server Quicktime Streaming Server Administration For Version 10.3 or Later
Provide identical operating system and applications folders for client computers	NetBoot	Mac OS X Server System Image Administration For Version 10.3 or Later
Install applications across a network	Network Install	Mac OS X Server System Image Administration For Version 10.3 or Later
Share information among multiple Mac OS X Servers or Mac OS X Computers	Directory services	Mac OS X Server Open Directory Administration For Version 10.3 or Later

Macintosh Manager

To manage Mac OS 9 client computers, you use Macintosh Manager, which you can use remotely from a Mac OS 9 or X computer.

For more information, see Chapter 10,"Using Macintosh Manager for Mac OS 9."

NetBoot

With NetBoot, Mac OS 9 and X computers can start up from a network-based system disk 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 NetBoot images, all computers using NetBoot have instant access to the new configuration.

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

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

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

You use several other applications to administer NetBoot:

- NetBoot Desktop Admin (for modifying Mac OS 9 images)
- Network Image Utility (for creating and modifying Mac OS X images)
- The DHCP/NetBoot module (used to save NetBoot images)

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

Network Install

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

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

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

For more information about using Network Install, read the system image administration guide.

Accounts

There are three basic kinds of accounts you can set up with Workgroup Manager: user accounts, group accounts (also called *workgroups*—two or more users with managed preferences), and computer lists.

When you define a user's account, you specify the information needed to prove the user's identity: user name, password, and user identification number (user ID). Other information in a user's account is needed by various services—to determine what the user is authorized to do and perhaps to personalize the user's environment. Mac OS X Server uses several different kinds of users and groups. Most of these are user-defined—user and group accounts that you create. There are also some predefined user and group accounts, which are reserved for use by Mac OS X.

Administrator Accounts

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

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

Server Administration

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

- A server administrator can use Server Admin and can make changes to a server's search policy using Directory Access.
- A server administrator can see *all* the AFP directories on the server (from a computer other than the server), not just share points.

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

Local Mac OS X Computer Administration

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

Directory Domain Administration

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 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 different users to be able to manage different groups.

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

Users and Managed Users

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

Most users have an individual account that is 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 the 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 preferences set up for any workgroup or computer list he or she belongs to. See Chapter 9, "Managing Preferences," and Chapter 10, "Using Macintosh Manager for Mac OS 9," for managed user information.

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 privileges set to Everyone. The guest user account is used when no matching user record is found during authentication.

Another kind of guest user is a managed user that you can define to allow easy setup of public computers or kiosk computers that use Mac OS 9. See Chapter 10, "Using Macintosh Manager for Mac OS 9," for more about these kinds of users.

Groups, Primary Groups, and Workgroups

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

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

Information in group accounts is used to help control user access to directories and files. See "Directory and File Access by Other Users" on page 30 for a description of how this works.

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 grant administration privileges for a group folder to a user. A group folder administrator has owner privileges for the group folder and can change group folder attributes in the Finder.

Workgroups

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

Any preferences you define for a Mac OS X workgroup are stored in the group account. Preferences for Mac OS 8 and 9 workgroups are stored using Macintosh Manager. See Chapter 9, "Managing Preferences," and Chapter 10, "Using Macintosh Manager for Mac OS 9," for a description of workgroup preferences.

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 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, Chapter 9, "Managing Preferences." For a description of how to set up computer lists and specify preferences for Mac OS 9 computers, Chapter 10, "Using Macintosh Manager for Mac OS 9."

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, or guest, computers.

A Guest Computers lists 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 User Experience

Once you have created an account for a user, the user can access server resources according to the privileges you have allowed. 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 is granted access to the server and network resources
- **Access** The user connects to and utilizes 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 access privileges allowed, the type of client computer (such as Windows or UNIX) currently in use, whether or not the user is a member of a group, and whether or not 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 8, "Client Management Overview." The Mac OS 9 user experience is described in Chapter 10, "Using Macintosh Manager for Mac OS 9." Basic information about authentication, password validation, and information access control is given in the sections that follow. For more detailed information about these topics, see the Open Directory administration guide.

Authentication

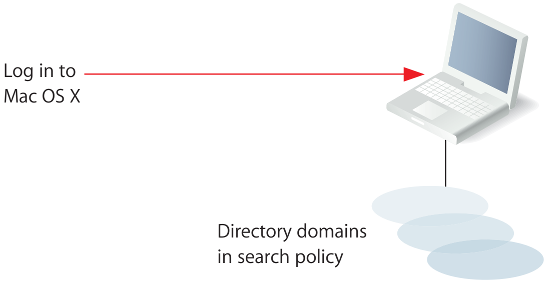
Before a user can log in to or connect with a Mac OS X computer, he or she must enter a name and password associated with a user account that the computer can find.

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

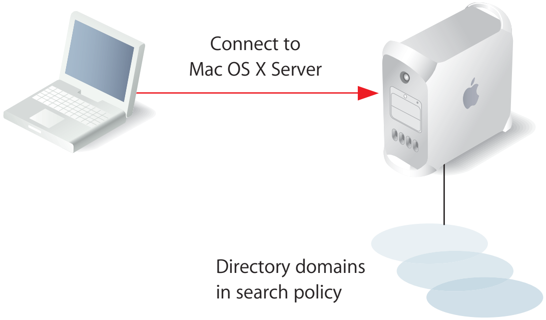
- A *directory domain* stores information about users and resources. It is like a database that a computer is configured to access in order to retrieve configuration information.
- A *search policy* is a list of directory domains the computer searches when it needs configuration information, starting with the local directory domain on the user's computer.

The 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.

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 of its search policy.



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



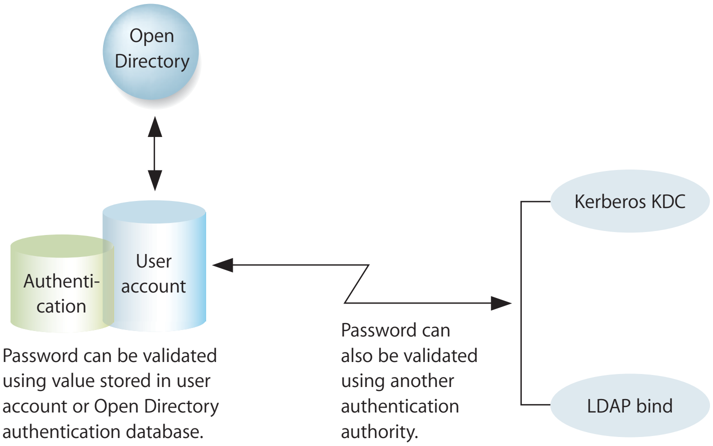
If Mac OS X finds a user account containing the name entered by the user, it attempts to validate the password associated with the account. If the password can be validated, the user is authenticated and the login or connection process is completed.

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

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

Identity Validation

When authenticating a user, Mac OS X first locates the user's account and then uses the password strategy designated in the user's account to validate the user's password.


Open Directory
User account
Authenti-cation
Kerberos KDC
LDAP bind
Password can be validated using value stored in user account or Open Directory authentication database.
Password can also be validated using another authentication authority.

Open Directory gives you several options for validating a user's password. For more details about password validation options, read the Open Directory administration guide.

Information Access Control

For any directory (folder) or file on a Mac OS X computer, you can specify access privileges for:

- the file's owner
- the file's group
- everyone else

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

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

Directory and File Owner Access

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

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

Directory and File Access by Other Users

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

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

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

Getting Started With User Management

2

This chapter provides information to use when first setting up a user management environment.

The chapter contains planning guidelines as well as tips for using the main user management tool, Workgroup Manager:

- The chapter starts with a setup overview to acquaint you with the sequence of major user management setup activities.
- Some planning strategies for user management appear on page 37.
- Basic instructions for using Workgroup Manager start on page 40.
- Instructions for listing and finding accounts in Workgroup Manager start on page 42.
- Some shortcuts for working with accounts are provided starting on page 45.
- Finally, page 46 addresses backing up and restoring user management files.

Setup Overview

This section provides an overview of user management setup tasks, including instructions for where to find detailed instructions:

- Step 1: Before you begin, do some planning.
- Step 2: Set up the server infrastructure.
- Step 3: Set up an administrator computer.
- Step 3: Set up a home directory share point.
- Step 4: Create user accounts and home directories.
- Step 5: Set up client computers.
- Step 6: Define user account preferences.
- Step 7: Create group accounts and group folders.
- Step 8: Define group account preferences.
- Step 9: Define computer lists and preferences.
- Step 10: Perform ongoing account maintenance.

Step 1: Before you begin, do some planning

Planning for user management includes such tasks as analysis of user needs and development of a directory services and home directory strategy. See "Planning Strategies for User Management" on page 37 for some suggestions.

Step 2: Set up the server infrastructure

The purpose of this step is to make sure that one or more Mac OS X Servers are set up for hosting user accounts, group accounts, computer lists, home directories, group folders, and other shared folders:

If you purchased a new server, Mac OS X Server software is already installed. All you need to do is perform initial server setup. Turn the computer on and answer the questions posed by Server Assistant. If you need to install server software, use the getting started guide to understand system requirements and installation options. Then use Server Assistant after the server restarts to perform initial server setup. Server Assistant resides in /Applications/Server/.

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. When you set up shared directories, client computers find it automatically, thanks to a few settings you make when setting up client computers (see step 6 on page 35). Users whose accounts reside in a shared directory are referred to as *network users*.

There are different kinds of shared directories and different ways to work with information stored in them. You can use Workgroup Manager to add and change accounts that reside in the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain. If you'll be using LDAPv2, read-only LDAPv3, BSD configuration files, or other read-only directories, make sure they are configured to support Mac OS X Server access and that they provide the data you need for accounts. It may be necessary to add, modify, or reorganize information in a directory to provide the information in the format needed.

The Open Directory administration guide provides instructions for setting up a shared directory on Mac OS X Server or configuring access to a shared directory on another computer. An appendix in the Open Directory administration guide describes account data formats that Mac OS X expects, information useful when you need to use directories that don't reside on Mac OS X Server computers.

If some of your users will be using Windows computers, see the Windows services administration guide to learn how to set up the server for managing Windows users, groups, and computers. For example, the Windows services administration guide describes how to set up user accounts in a Mac OS X Server directory domain so the server can provide file services, domain login, and home directories to Windows users.

Open Directory 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, Open Directory can access accounts in existing directories on your network, such as a Windows server's Active Directory. See the Open Directory administration guide for setup instructions.

Mac OS X Server makes other important resources visible throughout the network. Key network-visible resources include network home directories, group folders, and other shared folders. Because these folders reside on the server, users can access them from different computers.

See the file services administration guide for information about setting up file services appropriate for the file sharing you want to implement. You can use AFP or NFS for home directories, AFP for group folders, and various protocols (AFP, Windows, NFS, and FTP) for other shared folders.

Step 3: Set up an administrator computer

Because servers are normally kept in a secure, locked location, administrators conduct user management tasks remotely, from an administrator computer. Most of the time an administrator computer is a Mac OS X computer with server administration software installed.

To set up an administrator computer:

1 Obtain a computer with Mac OS X version 10.3 or later installed.

Make sure it has at least 128 MB of RAM and 1 GB of unused disk space.

2 Insert the Mac OS X Server Administration Tools disc, then start the installer (ServerAdmin.pkg).

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 similar.

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.

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 small globe above the accounts list.

Choose the directory of interest. If you're not authenticated, click the lock.

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 "User can 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 Rights for a Directory Domain" on page 67.

6 Click Save.

Now the remaining steps can be conducted by the domain administrator from the administrator computer.

Step 4: Set up a home directory share point

Home directories for accounts stored in shared directories can reside in a network share point that the user's computer can access. The share point must be *automountable*—it must have a network mount record in the directory domain where the user account resides.

An automountable share point ensures that the home directory is visible in /Network/Servers automatically when a user logs in to a Mac OS X computer configured to access the shared directory. It also lets other users access the home directory using the ~*home-directory-name* shortcut.

You can set up network home directories so they can be accessed using either AFP or NFS. You can also set up home directories for use by Windows users:

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

Step 5: Create user accounts and home directories

You can use Workgroup Manager to create user accounts in directories that reside on Mac OS X Server and in non-LDAP directories that aren't read-only. 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 creating Mac OS X mobile user accounts, see Chapter 3, "User Management for Mobile Clients."
- See Chapter 7, "Setting Up Home Directories," for information about home directories.
- See "Working With Read-Only User Accounts" on page 57 for information about working with read-only accounts.

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

Mac OS 9 users can be managed using Macintosh Manager after you create accounts for them on the server. For details, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

Note: When a user uses both Mac OS 9 and Mac OS X computers, you can set up one computer account for the user in a shared directory. But be aware that the user will not be able to access the same set of group folders in both environments. Mac OS 9 and Mac OS X have unique group preferences and group folders.

Step 6: Set up client computers

Mac OS X Server can support users of Mac OS X, Mac OS 9, or Windows client computers.

For Mac OS X computers, configure the search policy of the computer so it can locate shared directory domains. See the Open Directory administration guide for instructions and supplemental information about search policies in onscreen help. Use the Automatic authentication option if you've set up a DHCP server to identify the location of the shared directory when it provides an IP address to Mac OS X client computers. Otherwise, use the Custom Path option to identify the server hosting the shared directory.

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

For Mac OS 9 computer requirements and setup, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

Windows workstations that will be used for Windows domain login must join the Mac OS X Server PDC just as you would set up workstations to join a Windows NT server's domain, as the Windows services administration guide explains.

If you have more than just a few Macintosh client computers to set up, consider using the Network Install feature of the NetBoot service to create a system image that automates client computer setup. See the system image administration guide for options and instructions.

Step 7: Define user account preferences

You can 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 8, "Client Management Overview," and Chapter 9, "Managing Preferences."

- For information about Mac OS 9 user preferences, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

Step 8: Create group accounts and group folders

You can use Workgroup Manager to create group accounts in directories that reside on Mac OS X Server and in non-Apple Open Directory domains that aren't read-only. Detailed instructions appear in various locations in this guide:

- For information about how to create Mac OS X group accounts, see Chapter 5, "Setting Up Group Accounts."

  Although some group information doesn't apply to Windows users, you can add Windows users to groups that you create. The procedures for managing group accounts for Windows users are the same as those for groups that contain only Mac OS X users.
- For information about working with read-only group accounts, see "Working With Read-Only Group Accounts" on page 83.
- For information about using groups for Mac OS 9 users, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

You can set up a group folder for use by group members. Use Workgroup Manager to define a share point for the group folder and associate the share point with the group. Create the group folder using the CreateGroupFolder command in the Terminal application. See "Working With Group Folder Settings" on page 86 for instructions.

For Mac OS X users, use Dock or Login preferences to make it easy to locate the group directory. For Windows users, share the group folder share point using SMB. Users can go to My Network Places (or Network Neighborhood) and access the contents of the group folder. Group folders for Mac OS 9 users are described in Chapter 10, "Using Macintosh Manager for Mac OS 9."

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 8, "Client Management Overview," and Chapter 9, "Managing Preferences."
- For information about Mac OS 9 workgroups, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

Step 10: Define computer lists and preferences

Use computer lists if you want to manage client Macintosh or Windows 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 8, "Client Management Overview," and Chapter 9, "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:

- See the sections later in this chapter starting with "Listing and Finding Accounts" on page 42 for information about locating existing accounts and shortcuts for maintaining them.
- Information in Chapter 3 through Chapter 6 will help 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 11, "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 will access your network
- The kind of computers users will use (Mac OS 9, Mac OS X, or Windows)
- How users will 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 migration 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 all the domains have not 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, described in the Appendix, "Importing and Exporting Account Information."

Using Client Management

Take advantage of Macintosh client management if you want to:

- Provide users with a consistent, controlled interface while allowing them access to their files from any computer
- Use mobile accounts
- Reserve certain resources for only specific groups or individuals
- Secure computer usage 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 8, "Client Management Overview," Chapter 9, "Managing Preferences," and Chapter 10, "Using Macintosh Manager for Mac OS 9," for planning guidelines.

Using Mobile Accounts

Determine whether mobile accounts might be useful.

Mobile accounts are well suited for users who carry their computers from location to location. But they're useful for *any* users who don't require ongoing access to the server for their day-to-day work. Using mobile accounts reduces network traffic by minimizing the need to mount network resources (such as network home directories).

Mobile accounts are documented in Chapter 3, "User Management for Mobile Clients."

Devising a Home Directory Strategy

Determine which users need home directories and identify the computers on which you want user home directories to reside. For performance reasons, avoid using network home directories over network connections slower than 100 Mbps.

A user's network home directory 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 directories among various servers can help you balance your network workload. "Distributing Home Directories Across Multiple Servers" on page 104 describes several such scenarios.

You may want to store home directories for users with last names from A to F on one computer, G to J on another, and so on. Or you may want to store home directories on a Mac OS X Server but store user and group accounts on an Active Directory or LDAP server.

Pick a strategy before creating users. You can move home directories, but if you do, you may need to change a large number of user records.

Determine the access protocol to use for the home directories. Most of the time you will use AFP because it offers the greatest security. But you can use NFS (useful for UNIX clients) and SMB (for Windows clients).

Identifying Groups

Identify users with similar requirements and consider assigning them to groups.

For Mac OS X users, see Chapter 5, "Setting Up Group Accounts." For Mac OS 9 users, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

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) administrative privileges within certain directory domains.

Give some thought to which users require domain administrative privileges. Managed users can be given various administrative 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 administration privileges can help you distribute system administration tasks and make workflows 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 knowledge of 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 extreme caution and stored in a secure location. The root user has full access to the system, including system files. If you need to, you can use Workgroup Manager to change the root password.

Using Workgroup Manager

Once you have installed the Mac OS X Server software, you can access Workgroup Manager. This section provides an introduction to the application.

Opening and Authenticating in Workgroup Manager

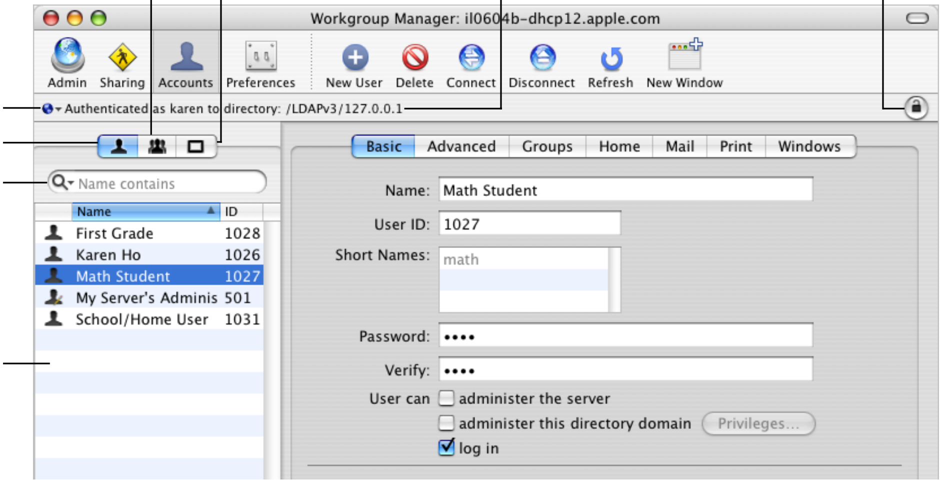
Workgroup Manager is installed in /Applications/Server/ when you install your server or set up an administrator computer. You can open it from that folder by using the Finder. You can also open Workgroup Manager by clicking its icon in the Dock or in the toolbar of the Server Admin application.

- 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 servers. Specify the user name and password for an administrator of the server, then click Connect. Use this approach when you'll be working most of the time with a particular server.
- To open Workgroup Manager on the server you're using without authenticating, choose View Directories from the Server menu. You will have read-only access to information displayed in Workgroup Manager. To make changes, click the lock icon to authenticate as an administrator. This approach is most useful when you'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 user account window appears, showing a list of user accounts.



Groups button

Computer Lists button

Currently selected domain

Click to be authenticated.

Click small globe to switch directories.

Users button

Type here to search or filter the list below.

Accounts list

Authenticated as karen to directory: /LDAPv3/127.0.0.1

Name	ID
First Grade	1028
Karen Ho	1026
Math Student	1027
My Server's Admins	501
School/Home User	1031

Name: Math Student

User ID: 1027

Short Names: math

Password: ••••

Verify: ••••

User can □ administer the server

□ administer this directory domain

☑ log in

Initially, the accounts listed are those stored in the last directory domain of the server's search path. Here is how to get started with the major tasks you perform with this application:

- To specify the directory or directories that store accounts you want to work with, click the small 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 list 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, respectively.
- To retrieve online information, 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 toolbar. See the getting started guide for information about Server Admin.

Listing and Finding Accounts

This section tells you about the various ways to 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 at 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 whether system users and groups are listed and the order in which items are listed. Choose Workgroup Manager > Preferences to set up Workgroup Manager preferences.
- The list reflects the directory or directories you select using the small globe above the accounts list. Initially, the parent directory domain accounts are listed if you're connected to the network.

  The domains available for selection are the local directory, all directory domains in the server's search path, and all available directory domains (domains the server is configured to access which may or may not be in the search path). See the Open Directory administration guide for instructions for configuring a server to access directory domains.

  After you choose directory domains, all the accounts residing in those domains are listed.
- 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 filter the list by using the pop-up search list above the accounts list.
- You can search for specific items in the list by typing in the field above the accounts list.

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 upon 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. Therefore, a server's file service can authenticate users with accounts from the server's local directory. 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, then click the small globe above the accounts list 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 (the leftmost button above the search field). Click the Groups button (the middle button) to view group accounts, and click the Computer Lists button (the rightmost) to view computer lists.

3 To work with a particular account, select it. To change the account, which requires that you have domain administrator privileges, you may need to click the lock to authenticate.

Listing Accounts in Search Path Directory Domains

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

To list accounts in search path 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 small globe above the accounts list and choose Search Path.

3 To view user accounts, click the Users button (the leftmost button above the search field). Click the Groups button to view group accounts, and click the Computers button to view computer lists.

Listing Accounts in Available Directory Domains

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

Note that "available" directory domains are not the same as directory domains in a search policy. A search policy consists of the directory domains a server searches routinely when it needs to retrieve, for example, a user's account. 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 the directory domains of interest are accessible.

2 Click the small globe above the accounts list and choose Other.

3 In the dialog that appears, select the domain(s), then click OK.

To view user accounts residing in selected directory domains click the Users button (the leftmost button above the search field). Click the Groups button to view group accounts, and click the Computer Lists button to view computer lists.

4 To work with a particular account, select it. To change an account that requires you to have domain administrator privileges, you may need to click the lock to authenticate.

Refreshing Account Lists

If more than one administrator can make changes to directories, 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, you can:

- 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 small globe above the accounts list and choose another item in the list, and then reselect the domain(s) with which you had been working.

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 pop-up menu above the account list (labeled with a magnifying glass), select an option to describe what you want to find, then type search terms in the text 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 or 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 filter field is empty, no accounts are listed.

To list all accounts in the domains selected in the At pop-up menu, type "*" in the filter field.

To list accounts in those domains that satisfy filter criteria, select an option from the pop-up menu next to the filter field, then enter a filter string.

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 as many as 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 order of the entries in the list.

Shortcuts for Working With Accounts

There are a several techniques that let you 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.

Batch Editing

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. Multi-account editing is referred to as *batch editing.*

To select multiple accounts, press Shift-click to select a range of accounts and/or Command-click to select accounts individually. You can also choose Edit > Select All, then Command-click to deselect accounts individually.

An example of when batch editing can save you time is when you need to change preference settings for large numbers of accounts. See "Editing Preferences for Multiple Records" on page 131.

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.

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 this way can make it easier to set up large numbers of accounts quickly. Exporting information to a file can be useful for record keeping or backing up user data.

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

Backing Up and Restoring User Management Data

Backing Up and Restoring Files

See onscreen help for information about backing up and restoring directory domains and authentication database files.

Backing Up Root and Administrator User Accounts

System files are owned by root or system 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 as described in the Appendix, "Importing and Exporting Account Information."

User Management for Mobile Clients

3

This chapter provides suggestions for managing portable computers used by an individual user or multiple users.

Setting Up Mobile Clients

If you have the advantage of owning a number of portable computers slated for distribution to specific users or groups of users, you can implement a variety of management techniques to personalize the user environment and control the level of access a user has to both local and network resources.

Configuring Portable Computers

In preparing portable computers for use on your network, follow these guidelines.

Step 1: Install the OS, applications, and utilities

Most computers will already have an operating system installed. However, if you need to install a new one, be sure the computers meet the minimum requirements for installation of the operating system (either Mac OS X or Mac OS 9) and any additional applications or utilities you want to install.

Step 2: Create local accounts on Mac OS X computers

Create at least one local administrator account and any local user accounts as needed. Make sure the user's local account name and password is not easily confused with the user's network name and password. Mac OS 9 doesn't require this step.

Step 3: Set up computer lists on your server

For Mac OS X computers, use Workgroup Manager to add the computers to a computer list and enforce preference management at the computer level. You may also want to set user-level preference management settings for the user's network account.

Details about configuring directory services are in the Open Directory administration guide. For more information about how to work with computer lists, see Chapter 6, "Setting Up Computer Lists." For additional information and instructions about using managed preference settings, see Chapter 9, "Managing Preferences."

For Mac OS 9 computers, use Macintosh Manager to set up computer lists and enforce preferred settings. To learn more about using Macintosh Manager, see Chapter 10, "Using Macintosh Manager for Mac OS 9."

Using Mobile Accounts

A mobile account is a Mac OS X Server user account that has been copied to a local (usually portable) computer. The user may log in on the portable computer using the network account name and password, even if the computer isn't connected to the network.

When a mobile account logs in to the network, account data—the account name, password, and managed preferences—is automatically synchronized with the server account so that both locations contain a matching set of data. (Mobile account users may want to manually copy files from their local home directory to the network home directory so that they may be accessed from other computers.) When the computer is disconnected from the network, any managed preference settings applied remain in force.

The home directory for the mobile account resides on the user's computer, whereas the home directory for the network account resides on the server. When the computer is connected to the network, the user authenticates directly to the server account, bypassing the mobile account but still using a local home directory.

If users mainly use a mobile account, their AFP network home directory is created the first time they attempt to access their network home directory. You can create a shortcut to provide mobile users with easy access to their network home directory (see "Providing Access to a User's Network Home Directory" on page 157). If you have mobile account users accessing a server hosting non-AFP network home directories, you need to create those network home directories manually (see Chapter 7, "Setting Up Home Directories," on page 103).

Creating a Mobile Account

Once a mobile account is created, it appears in the account list in the Accounts system preference. The account type is labeled "Mobile," and when you select it, most items in the Accounts pane are dimmed. You can use Workgroup Manager to create a mobile account automatically when a user logs in.

To create a mobile account using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select a user account, then click Preferences.
3. Click Mobile Accounts and set the management setting to Always.
4. Select "Create Mobile Account at login."

5 Select "Require confirmation before creating a mobile account" if you want to allow the user to decide whether to create a mobile account at login.

If this option is selected, the user sees a confirmation dialog when logging in. The user can click Create to create the mobile account immediately, or can click Continue to log in as a network user without creating the mobile account.

6 Click Apply Now.

You can use Workgroup Manager to make changes to the corresponding server account as needed. Any changes are applied to the mobile account the next time the user connects the portable computer to the network.

Deleting a Mobile Account

If a user no longer requires a mobile account, you can delete the account. Both the mobile account and its local home directory are deleted. You must have a local administrator account and password to delete a mobile account.

To delete a mobile account:

1 Open System Preferences on the client computer.

2 Click Accounts, then select the user in the list.

3 Select the account you want to delete.

The mobile account should have the word "Mobile" listed in the Type column.

4 Click the Delete (–) button, then click OK.

The User Experience for Mobile Accounts

If the computer is configured to display a list of users at login, the mobile account is displayed with local users. The user selects his or her account and then enters the correct password to complete login. For managed clients, if the network administrator has designated mobile accounts to be created at login for a particular user, group, or computer, the login window account list displays all users. After the user selects his or her account and types the correct password, a local cached network account is created immediately, behind the scenes. The user can now disconnect from the network and log in using his or her mobile account.

Managing Mobile Clients

After setting up the portable computers, you can use various features of Workgroup Manager or Macintosh Manager to apply restrictions or permit access to network services for users.

If a user has a network account and the computer is recognized by Open Directory, the user can log in using the network account name and password to gain access to available resources. For optimum performance, be sure Mac OS X computers are configured to use DHCP (in the Network pane of System Preferences) and an automatic search policy (in the Authentication pane of Directory Access). This is the default configuration for Mac OS X versions 10.2 and later. If you change the default configuration, users may experience delays in operating system performance when disconnected from the network. For more information about using DHCP and an automatic search policy to bind a computer to Open Directory service, see the Open Directory administration guide.

For users without network accounts who have portable computers of their own but still require access to your network resources, you can use Workgroup Manager or Macintosh Manager features to apply settings for unknown or guest computers.

Unknown Mac OS X Portable Computers

To manage users who have their own personal portable computers running Mac OS X system software, you can use the Guest Computers account to apply computer-level management for unknown or guest computers on your network. If these users log in using a Mac OS X Server user account, user and group managed preferences and account settings also apply.

For more information about setting up the Guest Computers account for Mac OS X users, see "Managing Guest Computers" on page 99. For information about managing unknown portable computers that use Mac OS 9 system software, see "Providing Quick Access to Unimported Users" on page 191.

Mac OS X Portable Computers With Multiple Local Users

One example of shared portable computers is an iBook Wireless Mobile Lab. An iBook Wireless Mobile Lab contains either 10 or 15 student iBooks (plus an additional iBook for an instructor), an AirPort Base Station, and a printer, all on a mobile cart. The cart lets you take the computers to your users (for example, from one classroom to another).

To manage the iBooks on your cart, create identical generic local user accounts on each computer (for example, all the accounts could use "Math" as the user name and "student" as the password). You might want to create different generic local accounts for different purposes, such as an account for a History class, one for a Biology class, and so on. Each account should have a local home directory and should not have administrative privileges. Use a separate local administrator account on each computer to allow server administrators (or other individuals) to perform maintenance tasks and upgrades, install software, and administer the local user accounts.

After creating the local user accounts, add each of the computers to a computer list, then manage preferences for that list. Because multiple users can store items in the local home directory for the generic account, you may want to periodically clean out that folder as part of your maintenance routine.

You can also create mobile accounts for users or use Workgroup Manager preference management to create a mobile account automatically when a user logs in.

Mac OS X Portable Computers With One Primary Local User

There are two ways set up portable computers for a single user who doesn't use a mobile account.

- **The user doesn't have administrator privileges, but has a local account.**

  Set up a local administrator account on the computer (don't give the user any information about this account), then set up a local account for the user. Users with local accounts that don't have administrator privileges can't install software and can add or delete items only in their own home directories. A local user can share items with other local users by using the Public folder in his or her local home directory.

  If this user had a mobile account, it would function as a local account but could be managed like a network account. If the user has an existing network account, you can change managed preference settings so that a mobile account is created during the user's first login.

- **The user is the administrator for the computer.**

  If the user is the local administrator, he or she can choose during login whether or not to be managed. For example, to access servers at school, the user should choose to be managed at login, but at home the user may prefer not to be managed since access to the school servers may not be available.

  If the user also has a Mac OS X Server user account and network access is available, it may still be preferable to log in using the local account to reduce network traffic. The user can connect to his or her network home directory (to store or retrieve documents, for example) via the "Go to Folder" command in the Finder's Go menu.

Managing Mac OS 9 Portable Computers

You can set up and manage portable computers that use Mac OS 9. Users can have either network accounts or local user accounts. Macintosh Manager has a "check out" feature that allows users to take home an assigned portable computer and work while not on a managed network.

For details about using Macintosh Manager to manage portable computers, see "Managing Portable Computers" on page 223.

Using Wireless Services

You can provide wireless network service to managed clients using AirPort, for example. When a user with a portable computer leaves the wireless area or changes to a different network directory server (by moving out of one wireless area and into another), client management settings may be different. Users may notice that some network services, such as file servers, printers, shared group volumes, and so forth, are unavailable from the new location. Users can purge these unavailable resources by logging out and logging in again.

If you need more information about using AirPort, consult AirPort documentation or visit the website: www.apple.com/airport/.

Setting Up User Accounts

4

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

About User Accounts

A user account stores data that Mac OS X Server needs to validate the user's identity and provide services for 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 the Mac OS X computer that needs access to the account. 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, an LDAP or Active Directory server).

You can use Workgroup Manager to work with accounts in all kinds of directory domains, but you can update only the LDAP directory of an Open Directory master, a NetInfo domain, or other read/write directory domain using Workgroup Manager.

See the Open Directory administration guide for complete information about the different kinds of Open Directory domains.

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).

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.
Macintosh Manager User	mmuser	-17	The user created by Macintosh Management Server when the application is first started on a particular server. This user has no home directory, and the password is changed periodically.
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	The user that is used when the system doesn't know about the hard disk.
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 to create a new user account in it.

To create a user account:

1 In Workgroup Manager, click Accounts.

2 Ensure that the directory services of the Mac OS X Server you're using has been configured to access the domain of interest.

See the Open Directory administrator's guide for instructions.

3 Click the small globe above the accounts list, then choose the domain in which you want the user's account to reside.

For example, 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.

5 Choose Server > New User or click New User in the toolbar.

6 Specify settings for the user in the tabs provided.

See "Working With Basic Settings for Users" on page 61 through "Working With Print Settings for Users" on page 75 for details.

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 59 and Appendix, "Importing and Exporting Account Information."

Creating Read-Write LDAPv3 User Accounts

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

To create an LDAPv3 user account:

1 In Workgroup Manager, click Accounts.

2 Ensure that the directory services of the Mac OS X Server you're using has been configured to use the LDAP server for user accounts.

See the Open Directory administration guide for details about how to use Directory Access to configure an LDAP connection and Appendix, "Importing and Exporting Account Information," for information about the user account elements that may need to be mapped.

3 Click the small globe above the accounts list, then choose the LDAPv3 domain in which you want the user's account to reside.

4 To authenticate, click the lock.

5 Choose Server > New User or click New User in the toolbar.

6 Specify settings for the user in the tabs provided. See "Working With Basic Settings for Users" on page 61 through "Working With Print Settings for Users" on page 75 for details.

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 59 and Appendix, "Importing and Exporting Account Information."

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 has been configured to access the desired directory domain.

See the Open Directory administrator's guide for instructions.

3 Click the small globe above the accounts list, then choose the domain in which the user's account resides.

4 To authenticate, click the lock.

5 Click the Users button and select the user.

6 Edit settings for the user in the tabs provided. See "Working With Basic Settings for Users" on page 61 through "Working With Print Settings for Users" on page 75 for details.

Editing Multiple Users Simultaneously

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

To edit multiple users:

1 In Workgroup Manager, click Accounts.

2 Select the user accounts you want to change.

Click the globe icon below the toolbar and choose the directory domain, and Command-click to select each user.

3 To authenticate, click the lock.

4 Click to display the pane you want to work with and make desired changes in fields that Workgroup Manager lets you update.

Modifying Accounts in an Open Directory Master When You're a Domain Administrator But Not a Server Administrator

If you are authorized to administer a directory domain but not the server, you can still modify accounts.

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 small globe icon above the accounts list and choose Other from the pop-up menu.

5 Open the directory domain you want to administer, and then click the lock to be authenticated as a 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 you're using has been configured to access the directory domain in which the account resides.

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

3 Click the small globe above the accounts list and choose the directory domain in which the user's account resides.

4 Use the tabs provided to review the user's account settings.

See "Working With Basic Settings for Users" on page 61 through "Working With Print Settings for Users" on page 75 for details.

Defining a Guest User

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 anonymous users:

- Windows services (see the Windows Services guide for information about configuring guest access)
- Apple file service (see the file services administration guide for information about configuring guest access)
- FTP service (see the file services administration guide for information about configuring guest access)
- Web service (see the web technologies administration guide for information about configuring guest access)

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

Another kind of guest user is a managed user that you can define to allow easy setup of public computers or kiosk computers. See Chapter 9, "Managing Preferences," and Chapter 10, "Using Macintosh Manager for Mac OS 9," for more about these kinds of users.

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.

> *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.

   To locate the account, click the small globe above the accounts list and choose the directory domain where the account resides, then select the user.
3. To be authenticated, click the lock.
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 on 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 (for a user account whose password type is Open Directory).

Working With Presets for User Accounts

Presets are like templates with which you 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 will be creating user accounts.

   Ensure that the server has been configured to access the Mac OS X directory domain or non-Apple LDAPv3 domain in which the preset will be used to create new accounts. To access a different domain, click the small globe above the accounts list.

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 directory settings, quotas, default shell, primary group ID, group membership list, comment, login settings, print settings, and mail settings.

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, 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 the preset will be used to create the new account.

2. Click Accounts.

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

4 To authenticate, click the lock.

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

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.

Changing Presets

When you change a preset, existing accounts created using it are not updated to reflect your changes.

To change a preset:

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

2 Click 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, 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 for Users

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 Long User Names

The user name is the long name for a user, such as Ellen Brown or Dr. Arnold T. Smith. 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.

Long user names are case-sensitive in the login window; so if an account has the user name Mary Smith, login fails if MARY SMITH is entered in the login window. However, user names are not case-sensitive when used to authenticate a user for file server access or to log in from Macintosh Manager Mac OS 9 clients.

A long 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.
3. To be authenticated, click the lock.
4. In the Name field (on the Basic pane), review or edit the user name.

   Initially, the value of user name is "Untitled <some-number>." 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 path (search policy) of the server you're using, but has no way of detecting whether duplicates might exist in other domains.

Defining Short User Names

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

- When Mac OS X automatically creates a user's local or network AFP home directory, it names the directory after the user's short name. For more information about home directories see Chapter 7, "Setting Up Home Directories."
- When Mac OS X checks to see whether a user belongs to a group authorized to access a particular file, it uses short names to find user IDs of group members. See "Avoiding Duplicate Short Names" on page 64 for an example.

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 directories and 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)
- - (hyphen)

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 small globe above the accounts list and choose the directory domain where the account resides, then select the user account.
3. To be authenticated, click the lock.
4. In the Short Names field (on the Basic pane), review or edit the short names.

Initially, the value of the short name is "untitled_<some-number>." If you specify multiple short names, each should be on its own line.

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 path (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

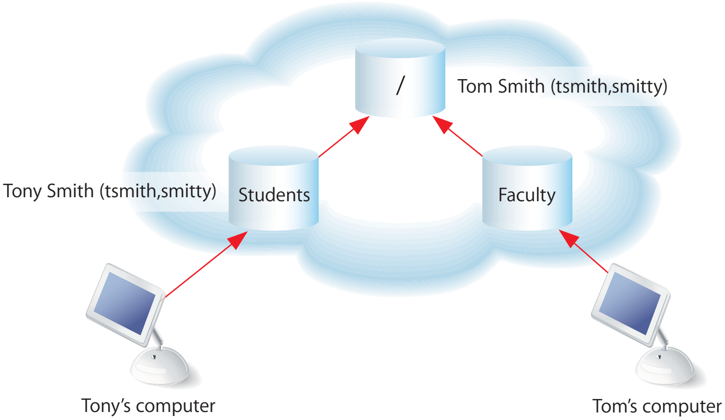
When you create groups, Mac OS X identifies users in them by their first short name, which can't be changed.

If a short name change is unavoidable, you can create a new account for the user (in the same directory domain) that contains the new short name, but retains all other information (user ID, primary group, home directory, 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 58 for information on disabling use of an account for login.)

Avoiding Duplicate Names

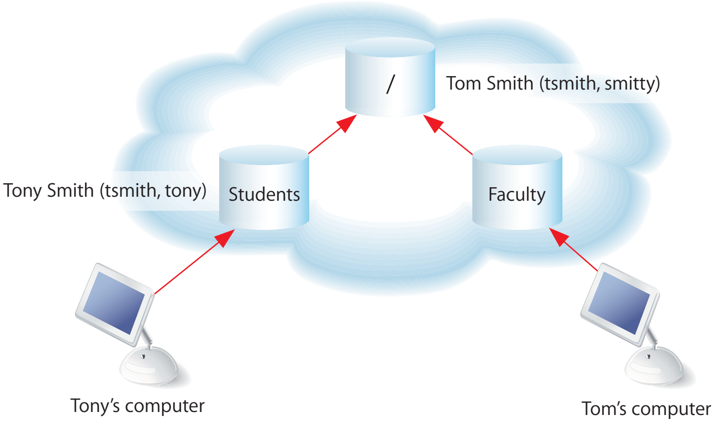
If separate user accounts have the same name (user name or short name) and password, a Mac OS X computer may authenticate a user different from the one you want it to authenticate. Or it may mask the user record that should be used for authentication.

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



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

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



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

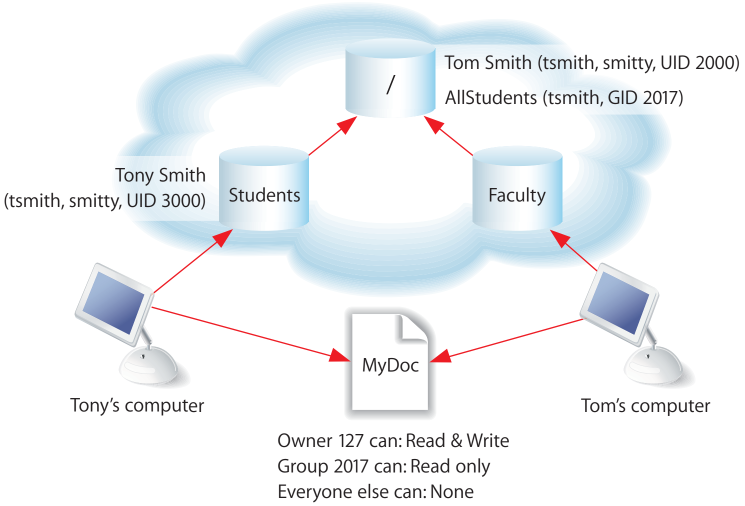
If Tony has a user record in his local directory domain that has the same names and password as his record in the Students domain, the Students domain's record for Tony would be masked. Tony's local domain should offer a name/password combination that distinguishes it from the Students domain's record.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

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

Avoiding Duplicate Short Names

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

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


/
Tom Smith (tsmith, smitty, UID 2000)
AllStudents (tsmith, GID 2017)
Tony Smith
(tsmith, smitty, UID 3000)
Students
Faculty
MyDoc
Tony's computer
Tom's computer
Owner 127 can: Read & Write
Group 2017 can: Read only
Everyone else can: None

Now suppose that a file, MyDoc, resides on a computer accessible to both Tony and Tom. The file is owned by a user with the user ID 127. It has read-only access privileges for AllStudents. Tony, not Tom, was added as a member of AllStudents, but because a group's member list consists of short names, not user IDs, and the short name tsmith is listed as a member of AllStudents, both Tony and Tom are effectively members of AllStudents.

When Tom attempts to access MyDoc, Mac OS X determines that the owner permissions do not apply for Tom, and moves on to check if group permissions apply for Tom. Mac OS X searches the login hierarchy for user records with short names that match those associated with AllStudents. Tom's user record is found (short name tsmith) because it resides in the login hierarchy, and the user ID in the user record is compared with Tom's login user ID. They match, so Tom is allowed to read MyDoc, even though he's not actually a member of AllStudents.

Defining User IDs

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

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

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.

In general, once user IDs have been assigned and users start creating files and directories throughout a network, 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 into 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 path. (New users created using the Accounts Preferences pane on Mac OS X Desktop computers 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 small 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.

4 In the Basic pane, specify a value in the User ID field.

Make sure the value is unique in the search policy (search path) of computers the user will log in to.

Defining Passwords

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

Setting Password Options for Imported Users

You can't set Open Directory password options in an import file or in a preset used during import.

To set password options for imported users:

1 Import the users by using Workgroup Manager or the `dsimportexport` command-line tool.

2 In Workgroup Manager, click Accounts.

3 Open the directory into which the users were imported.

4 Select the users whose password options you want to set.

5 Click Advanced.

6 Make sure the User Password Type is set to Open Directory, click Options, set password options, and click OK.

7 Click Save.

For more information about importing users, see the appendix. For additional information about Open Directory passwords, see the Open Directory administration guide.

Assigning Administrator Rights for a Server

A user who has server administration privileges can control most of the server's configuration settings and use applications, such as Server 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 small globe above the accounts list and choose the directory domain in which the user's account resides.

4 To authenticate, click the lock.

5 In the Basic pane, select "User can administer the server" to grant server administrator privileges.

Assigning Administrator Rights 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 for 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 small globe above the accounts list and choose the directory domain in which the user's account resides, and select the account.

4 To be authenticated, click the lock.

5 In the Basic pane, select "User can administer this directory domain."

6 To specify what the user should be able to 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 not change it.

To add an item 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 on the keyboard.

Working With Advanced Settings for Users

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

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.
- Indicate whether a user of a managed computer can or must select a workgroup during login or whether you want to avoid showing workgroups when the user logs in.
- Identify the default shell the user will use for command-line interactions with Mac OS X, such as /bin/csh or /bin/tcsh. The default shell is used by the Terminal application on the computer the user is logged in to, but Terminal has a preference that lets you override the default shell. The default shell is used by SSH (Secure Shell) or Telnet when the user logs in to a remote Mac OS X computer.

You can use Workgroup Manager to define login settings of an account stored in 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 in 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 small globe above the accounts list and choose the directory domain where the account resides, and select the user in the user list.

3 To be authenticated, click the lock.

4 Click Advanced.

5 Select "Allow simultaneous login" to let a user 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 directory, 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 cannot disable simultaneous login for users with NFS home directories.

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.

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 a command line, choose None.

Defining a Password Type

For details about setting up and managing passwords, see the Open Directory administration guide.

Creating a Master List of Keywords

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

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 apply 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 small globe above the accounts list and choose the directory domain where the account resides, and select the user in the user list.

3 To be authenticated, click the lock.

4 Click Advanced.

5 Click Define 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, type terms in the text field and click (+).

7 To remove a keyword from the master list and all user records where it appears, select the keyword, select Remove Deleted Keywords From Users, and click (–).

If you only want to remove a keyword from the master list, make sure Remove Deleted Keywords From Users is not selected, then select the keyword you want to remove and click (–).

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 at a time; however, you can remove a keyword from all users 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Advanced.

5 To add a keyword to the selected account, Click (+) to view the list of available keywords. Select one or more terms in the list, then click OK.

6 To remove a keyword from a specific user, select the term you want to remove and click (–).

7 When you've finished adding or removing keywords for the selected user, 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Advanced.

5 Edit or review the contents of the Comment field.

Working With Group Settings for Users

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

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

See Chapter 5, "Setting Up Group Accounts," for information on administering groups.

Defining a User's Primary Group

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

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

The primary group ID should be a unique string of digits. By default, it is 20 (which identifies the group named "staff"), but you can change it. The maximum value is 2,147,483,648.

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

3 To be authenticated, click the lock.

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 path 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 access privileges or when you want to manage their Mac OS X preferences using workgroups or computer lists.

You can use Workgroup Manager to add a user to a group if the user and group accounts are in 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 user account you want to work with.

   To select the account, click the small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.
3. To be authenticated, click the lock.
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. (To include system groups in the list, choose Preferences on the Workgroup Manager menu, then select "Show system users and groups.")
6. Select the group, then drag it into the Other Groups list on the Groups pane.

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

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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.
3. To be authenticated, click the lock.
4. Click the Groups button.
5. Select the group or groups from which you want to remove the user, 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

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 for Users

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

Working With Mail Settings for Users

You can create a Mac OS X Server mail service account for a user by specifying mail settings for the user in the user's account. To use the account, the user 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 account 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.

Disabling a User's Mail Service

You can use Workgroup Manager to disable mail service for a user whose account is 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Mail.

5 Select None.

Enabling Mail Service Account Options

You can use Workgroup Manager to enable mail service and set mail options for a user account stored in 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

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 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.

Forwarding a User's Mail

You can use Workgroup Manager to set up email forwarding for a user whose account is 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.
3. To be authenticated, click the lock.
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 for Users

Print settings associated with a user's account define the ability of a user to print to accessible Mac OS X Server print queues for which print service enforces print quotas. The print service administration guide tells you how to set up quota-enforcing print queues.

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

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

Disabling a User's Access to Print Queues Enforcing Quotas

You can use Workgroup Manager to prevent a user from printing to any accessible Mac OS X print queue that enforces quotas. To use Workgroup Manager, the user's account must be stored in 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Print.

5 Select None.

Enabling a User's Access to Print Queues Enforcing Quotas

You can use Workgroup Manager to allow a user to print to all or only some accessible Mac OS X print queues that enforce quotas. To use Workgroup Manager, the user's account must be stored in 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Print.

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 should be able to 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 for which you want to define a user quota. If the print queue you want to specify is not on the Queue Name pop-up menu, click Add to enter the queue name and specify, in the Print Server field, the IP address or DNS name of the server where the queue is defined.

To give the user unlimited printing rights to the queue, click "Unlimited printing." Otherwise, specify the maximum number of pages the user should be able to print in a certain number of days. Then click Save.

Deleting a User's Print Quota for a Specific Queue

If you no longer require a print quota for a particular queue, 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the list.

3 To be authenticated, click the lock.

4 Click Print.

5 Use the Queue Name pop-up menu and the Print Server field to identify the print queue to which you want to disable a user's access.

6 Click Delete.

Resetting a User's Print Quota

On some occasions, 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 her print quota is only 150 pages. Or, a student may exceed his 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 small globe above the accounts list and choose the directory domain where the account resides, then select the user in the user list.

3 To be authenticated, click the lock.

4 Click Print.

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 a print queue, then click Restart Print Quota.

You can also extend a user's page limit without resetting the quota 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.

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 guide.

Setting Up Group Accounts

5

A group account offers a simple way to manage a collection of users with similar needs. This chapter tells you how to set up and manage group accounts.

About Group Accounts

Group accounts store the identities of users who belong to the group as well as information that lets you customize the working environment for members of a group. 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.

Administering Group Accounts

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

Where Group Accounts Are Stored

Group accounts, as well as user accounts and computer lists, can be stored in any Open Directory domain accessible from the Mac OS X computer that needs to access the account. A directory domain can reside on a Mac OS X computer (for example, 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. See the Open Directory administration guide for complete information about the different kinds of Open Directory domains.

Predefined Group Accounts

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

Predefined group name	Group ID	Use
admin	80	The group to which users with administrator privileges belong.
bin	7	A group that owns all binary files.
daemon	1	A group used by system services.
dialer	68	A group for controlling access to modems on a server.
guest	31	
kmem	2	A legacy group used to control access to reading kernel memory.
mail	6	The group historically used for access to local UNIX mail.
mysql	74	The group that the MySQL database server uses for its processes that handle requests.
network	69	This group has no specific meaning.
nobody	-2	A group used by system services.
nogroup	-1	A group used by system services.
operator	5	This group has no specific meaning.
smmsp	25	The group used by sendmail.
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.
wheel	0	Another group (in addition to the admin group) to which users with administrator privileges belong.
www	70	The nonprivileged group that Apache uses for its processes that handle requests.

Creating Mac OS X Server Group Accounts

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

To create a group account:

1 In Workgroup Manager, click Accounts.

2 Ensure that the directory services of the Mac OS X Server you're using has been configured to access the domain of interest.

See the Open DIrectory administration guide for instructions.

3 Click the small globe above the accounts list and open the domain in which you want the group account to reside.

4 Click the lock to be authenticated as a directory domain administrator.

5 Click the Groups button.

6 Click New Group, then specify settings for the group in the tabs 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 the appendix.

Creating Read-Write LDAPv3 Group Accounts

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

To create an LDAPv3 group account:

1 In Workgroup Manager, click Accounts.

2 Ensure that the directory services of the Mac OS X Server you're using has been configured to use the LDAP server for group accounts.

See the Open Directory administration guide for information about using Directory Access to configure an LDAP connection and the appendix for information about the group account elements that may need to be mapped.

3 Click the small globe above the accounts list and open the LDAPv3 domain in which you want the group account to reside.

4 To be authenticated, click the lock.

5 Choose Server > New Group.

6 Specify settings for the group in the tabs provided.

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

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 the appendix.

Creating a Preset for Group Accounts

Group account presets can be used to apply predetermined settings to a new group account.

To create a preset for group accounts:

1. Open Workgroup Manager on the server from which you will be creating 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 will be 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 you're using has been configured to access the directory domain of interest.

   See the Open Directory administration guide for instructions.
3. Click the small globe above the accounts list and open the domain in which the group account resides.
4. To be authenticated, click the lock.
5. Click the Groups button and select the group you want to work with.
6. Edit settings for the group in the tabs provided.

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

Working With Read-Only Group Accounts

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

To work with a read-only group account:

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

   See the Open Directory administration guide for information about using Directory Access to configure server connections and the appendix for information about the group account elements that need to be mapped.
3. Click the small globe above the accounts list and open the directory domain in which the group account resides.
4. Use the tabs provided to review the group account settings.

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

Working With Member Settings for Groups

Member settings include a group's names, its ID, and a list of the users who are members of the group.

In Workgroup Manager, 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 access privileges or when you want to make them managed users.

When you create a user account and assign the new user a primary group, the user is automatically added to the group you specify; you don't need to explicitly do so. Otherwise, you explicitly add users to a group.

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

To add users 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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 Click Members.

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

6 To include system users in the list, choose Workgroup Manager > Preferences, then select "Show system users and groups."

Make sure that the group account resides in a directory domain specified in the search policy (search path) of computers the user will log in to.

7 Select the user, then drag it into the Members list on 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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 Click Members.

5 Select the user or users you want to remove from the group, 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 full group names support various character sets, the maximum number of characters for full 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 and 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, is 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.

You can use Workgroup Manager to edit the 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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 In the Name or "Short name" field (on 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.

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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 In the Group ID field (on 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

You can set up a folder for use by members of a particular group. A group folder offers a way to organize documents and applications of special interest to group members and gives group members a way to pass information back and forth among themselves.

To set up a group folder:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to work with.

To select an account, click the small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 Click the Groups button and select a group.

5 Click Group Folder.

6 To set up a group folder in a subfolder of a share point, click the Add (+) button or the Duplicate button (copy icon).

See "Creating a Group Folder in a Subfolder of an Existing Share Point" on page 90 for instructions.

Specifying No Group Folder

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

To define 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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.
3. To be authenticated, click the lock.
4. Click the Groups button and select a group.
5. Click Group Folder.
6. Select (None) in the list.

Creating a Group Folder in an Existing Share Point

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.

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 small globe above the accounts list and open the directory domain where the group account is stored, click the Groups button, and select the group.
3. To be authenticated, click the lock.
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 will be given read/write access to the group folder.

7 Click Save.

8 To create the folder, use the CreateGroupFolder command in Terminal.

You must be the root user to use the command. For more information, 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. See "Providing Easy Access to Group Folders" on page 141 for instructions.
- 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. See "Providing Easy Access to the Group Share Point" on page 158 for instructions.

When using 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 use the "Connect to Server" command in the Finder's Go menu to navigate to the server where the group folder resides to access the group folder.

Creating a Group Folder in a New Share Point

You can use Workgroup Manager to create a group folder in a new share point.

To create a group folder in a new share point:

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

2 In Workgroup Manager, connect with the server in step 1 and click Sharing.

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. Set Group privileges to Read & Write, set Everyone privileges to Read Only, and change the name in the Group field to "admin."

   Ignore the Owner privileges for now.

6. Click Save.

7. Click Accounts and select the group account you want to work with.

   To select a group account, connect to the server where the account resides. Click Accounts. Click the small globe above the accounts list and open the directory domain where the group account is stored. Click the Groups button and select the group.

8. To be authenticated, click the lock.

9. 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 will be given read/write access to the group folder.

10. To create the folder, use the CreateGroupFolder command in Terminal.

    You must be the root user to use the command. For more information, 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.

    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. See "Providing Easy Access to Group Folders" on page 141 for instructions.
- 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. See "Providing Easy Access to the Group Share Point" on page 158 for instructions.

When using 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 use the "Connect to Server" command in the Finder's Go menu to navigate to the server where the group folder resides to access the group folder.

Creating a Group Folder in a Subfolder of an Existing Share Point

In Workgroup Manager, you can 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.

The procedure detailed here assumes the share point exists. If the share point does not yet exist, follow the instructions in "Creating a Group Folder in a New Share Point" on page 88 but don't create the folder in the last step. Then follow the procedure here.

To set up a group folder in a subfolder of an 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 small globe above the accounts list and open the directory domain where the group account is stored, click the Groups button, and select the group.

3 To be authenticated, click the lock.

4 Click Group Folder.

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

To remove a group folder location, select it and click the Delete (–) button. You can delete only locations that were added with the Add or Duplicate buttons.

6 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."

7 In the Path field, enter the path from the share point to the group folder, including the group folder but excluding the share point.

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.

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

8 Click OK.

9 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 will be given read/write access to the group folder.

10 To create the folder, use the CreateGroupFolder command in Terminal.

You must be the root user to use the command. For more information, 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.

11 Set up access to the group folder for users who log in as group members.

- 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. See "Providing Easy Access to Group Folders" on page 141 for instructions.
- You can set up login preferences so users can click Computer in the Finder to see the group folder share point and the group folders within it. See "Providing Easy Access to the Group Share Point" on page 158 for instructions.

When using 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 use the "Connect to Server" command on the Finder's Go menu to navigate to the server where the group folder resides to access the group folder.

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 small globe above the accounts list and open 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.

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 small globe above the accounts list and open the directory domain where the account resides, click the Groups button, and select the group.
3. To be authenticated, click the lock.
4. Choose Server > Delete Selected Group or click the Delete icon in the toolbar.

Setting Up Computer Lists

6

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

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 two preset computer lists, Guest Computers and Windows Computers. These two lists, along with the computer lists that you set up, appear on the left side of the Workgroup Manager window. Settings appear on 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 will be included. 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 "on board," or built-in, Ethernet address, which is unique to each computer. (A computer's Ethernet address is also known as its *MAC address.*) You can browse for a computer and Workgroup Manager will enter 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. You don't need to know the Ethernet address of Windows client computers.

When a client computer starts up, directory services check for a computer list that contains the computer's Ethernet address, and uses preference information for that computer list. If no record is found, the client computer uses preference information for the Guest Computers computer list.

To edit computer lists or computer list preferences, you must have an administrator with privileges to edit computer lists. You can have administration privileges for all computer lists or for a set of specific computer lists. For more information about assigning administrative privileges, see Chapter 4, "Setting Up User Accounts."

Creating a Computer List

A computer list is a group of computers that have the same preference settings and are available to the same users and groups. You can use a computer list to assign the same 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 small globe above the accounts list and choose the directory domain where you want to store the new computer list.

3 To authenticate, click the lock.

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

5 Choose Server > New Computer List (or click New Computer List in the toolbar), then type a name for the computer list.

6 To use a preset, choose one from the Presets pop-up menu.

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 will enter 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 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 Add a comment (optional).

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 on 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 "Defining Preferences" on page 117 and Chapter 9, "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 small globe above the accounts list and choose the directory domain where you want to create a computer list using presets.
3. To authenticate, click the lock.
4. Click the Computer Lists button (on the left), 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 on 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 delete it or change its name.

To change a preset's name, choose the preset from the Presets pop-up menu, then choose Rename Preset.

To delete a preset, choose a preset from the Presets pop-up menu, then choose Delete Preset.

Using a Computer 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 switch the list to a different preset).

To use a preset for computer lists:

1. In Workgroup Manager, click Accounts.
2. Click the small globe above the accounts list and choose the directory domain where you want to store the new list.

3 To authenticate, click the lock.

4 Click the Computer Lists button (on the left), 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, 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 any computer that's 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 small globe above the accounts list and choose the directory domain that contains the list, click the Computer Lists button, and select the list.

3 To authenticate, click the lock.

4 Click List.

5 To use a preset, choose one from the Presets pop-up menu.

6 Click the Add (+) button and enter the requested information.

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

A computer's address must be the "on board," or built-in, Ethernet address, which is unique to each computer. (A computer's Ethernet address is also known as its *MAC address*.)

7 Add a comment (optional).

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.

8 Click Save.

9 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 when 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 small globe above the accounts list 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.

4 On 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 of a computer in the list to edit the information directly in the list.

5 Change information as needed, then click Save.

Moving a Computer to a Different Computer List

Occasionally, you may want 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 small globe above the accounts list 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.

4 On the List pane, select the computer you want to move and click the Edit (pencil) button.

5 Choose a list from the "Move to list" pop-up menu and click OK.

6 Click Save.

Deleting Computers From a Computer List

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

To delete 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 small globe above the accounts list 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.

4 On the List pane, select one or more computers.

5 Click the Remove (–) button, then click Save.

Deleting a Computer List

If you no longer need any computers 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 small globe above the accounts list 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.

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 search results.

To search for a computer list:

1 In Workgroup Manager, click Accounts, click the Computer Lists button (on the left), then click List (on the right).

2 To limit your search, click the small globe above the accounts list 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 path (for example, myserver.mydomain.com).

Other: Browse and select an available directory domain to search for computer lists.

3 To authenticate, click the lock.

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.

Managing 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, or "guest," computers.

A Guest Computers lists 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 small globe above the accounts list and choose the directory domain that contains the Guest Computers list you want to modify.

3 To authenticate, click the lock.

4 Click the Computer Lists button (on the left) and select Guest Computers in the list.

5 Click List (on the right), then select a setting for preferences.

To set up managed preferences, select "Define Guest Computer preferences here." If you select this option, click Save and continue with the next step.

To make guest computers have the same managed preference settings as the parent server (a server whose LDAP directory or shared NetInfo directory is listed in the search policy of the server you're configuring), select "Inherit preferences for Guest Computers." If you select this option, click Save; the next step is not necessary.

6 If you selected Define, click Access and select the settings you want to use. Click Cache, set an interval for clearing the preferences, 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 "Defining Preferences" on page 117 and Chapter 9, "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.

If the user has an administrator account in a client computer's local directory, the user can choose not to be managed at login. Unmanaged users can still use the "Go to Folder" command to access a home directory on the network.

Working With Access Settings

Settings in the Access pane let you make computers in a list available to users in groups. You can allow only certain groups to access computers in a list, or you can allow all groups (and therefore, all users) to access the computers in a list. You can also control certain aspects of local user access.

Restricting Access to Computers

You can reserve computers so that only certain users have access to them. 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.

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 small globe above the accounts list 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.
4. Click Access.
5. Select "Restrict to groups below."
6. Click the Add (+) button, 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.
7. Click Save.

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 small globe above the accounts list 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.
4. Click the Computer Lists button and select one or more computer lists.

5 Click Access.

6 Select "All groups can use the computer."

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 small globe above the accounts list 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.

4 Click Access.

5 Select an option to determine which workgroups are displayed when a local user logs in.

To let the user see a list of all available workgroups, select "All groups can use the computer."

To display only certain workgroups, select "Restrict to groups below," then drag groups from the drawer to the list in the Access pane.

6 Make sure "Allow users with local-only accounts" is selected.

7 Click Save.

Setting Up Home Directories

7

Mac OS X uses the home directory—a folder for a user's personal use—to store system preferences and managed settings. This chapter provides guidelines for setting up and managing home directories.

About Home Directories

You can set up home directories so they can be accessed using either Apple Filing Protocol (AFP) or Network File System (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 client IP address, so it is generally less secure than AFP. Use NFS only if you need to provide home directories for a large number of users who use UNIX workstations.

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

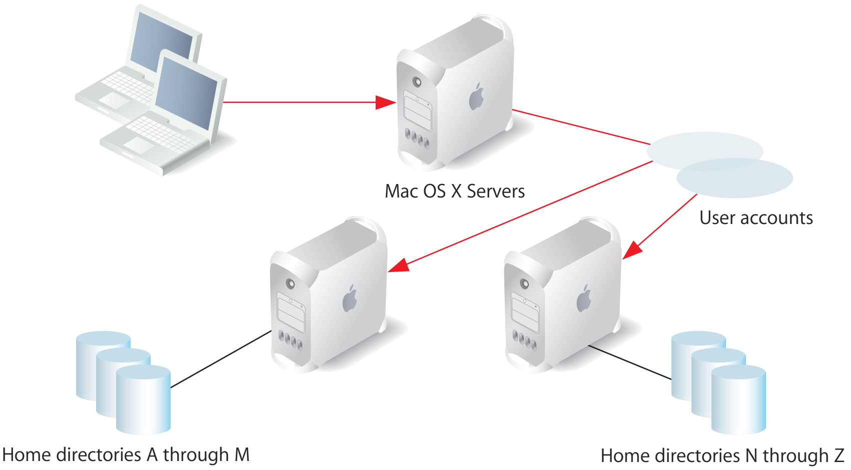
You can also import user home directory settings from a file. For an explanation of how to work with import files, see Appendix, "Importing and Exporting Account Information."

A user's home directory 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 directories among various servers can help you balance your workload among several servers. "Distributing Home Directories Across Multiple Servers" on page 104 describes several such scenarios.

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

Distributing Home Directories Across Multiple Servers

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



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

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

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 directories on each home directory server

Instructions later in this chapter tell you how to set up automountable share points.

Step 3: Create the user accounts in the shared domain on the accounts server

Instructions later in this chapter tell you how to set up accounts so that home directories reside in one or the other of the automountable share points.

See instructions in "Creating Mac OS X Server User Accounts" on page 55 to learn how to set user account attributes and subsequent sections of this chapter for details specific to home directory 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, if a home directory hasn't been created, the home directory is created automatically (if it hasn't already been created) on the appropriate server and is visible on the user's computer.

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

Specifying No Home Directory

You can use Workgroup Manager to change a user account that has a home directory to have none. By default, new users have no home directory.

To define no home directory:

1. In Workgroup Manager, click Accounts.
2. Open the directory domain in which the user account resides and authenticate as an administrator of the domain.

   To open a directory domain, click the small globe above the accounts list 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, then select None in the list.
5. Click Save.

Creating a Home Directory for a Local User

You can use Workgroup Manager to define home directories 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.

Home directories for local users should reside in AFP share points on the server where the users' accounts reside. These share points do not have to be automountable (they do not require network mount records).

To create a home directory for a local user account:

1. Make sure that a share point for the home directory exists on the server where the local user account resides.

You can use the predefined /Users share point or any other AFP share point that has been defined on the server. Alternatively, you can define your own share point. To use an existing share point, skip to step 4. To define a new share point, continue with steps 2 and 3.

Because of the way home directory disk quotas work, you may want to set up home directory share points on a partition different from other share points. See "Setting Disk Quotas" on page 113 for more information.

2 Using the Finder, create the folder you want to use as the share point if required.

3 In Workgroup Manager, connect to the server where the local user account resides and click Sharing to set up the folder as an AFP share point.

Click All (above the list on the left) and select the folder.

Click General and select "Share this item and its contents."

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.

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

Click Save.

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

To select a local user account, click the small globe above the user list and open the local directory domain, click the Users button, then select the user in the user 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 directory.

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

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

8 (Optional) Enter a disk quota and specify megabytes (MB) or gigabytes (GB).

9 Click Create Home Now, then click Save.

If you do not click Create Home Now before clicking Save, the home directory is created the next time the user restarts the client computer and logs in remotely. However, only certain clients (for example, Mac OS 9 clients connecting via Macintosh Manager) can connect to servers hosting sharepoints in the local domain. For instructions on setting up a share point for Mac OS X clients, see "Creating a Network Home Directory" on page 107.

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

10 Make sure AFP service is running on the server where the local user's home directory resides.

To check the status of AFP service, open Server Admin and connect to the server where the local user account resides. Select AFP in the Computers & Services list and click Overview. If the status indicates Apple File Service is stopped, choose Server > Start Service or click Start Service in the toolbar.

Creating a Network Home Directory

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

A user's network home directory can reside in any AFP or NFS share point that the user's computer can access. The share point must be automountable—it must have a network mount record in the directory domain where the user account resides. An automountable share point ensures that the home directory is visible in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain. It also lets other users access the home directory using the ~*home-directory-name* shortcut.

You can use Workgroup Manager to define a network home directory 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 directory information in any accessible read-only directory domain.

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

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

See "Setting Up an Automountable AFP Share Point for Home Directories" on page 110 or "Setting Up an Automountable NFS Share Point for Home Directories" on page 111 for instructions.

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 small globe above the accounts list and open the directory domain where the user account is stored. Click the Users button and select the user in the user list.

3 To be authenticated, click the lock.

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

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 path of the server you are connected to. 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 directories as described in step 1.

6 (Optional) Enter a disk quota and specify megabytes (MB) or gigabytes (GB).

7 Click Create Home Now, then click Save.

If you do not click Create Home Now before clicking Save, the home directory is created the next time the user restarts the client computer and logs in remotely.

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

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

8 Make sure that the user restarts his or her client computer so that the share point is visible on it.

Note that when the user logs in using SSH to obtain command-line access to the server, the user's home directory isn't mounted, and the user has only guest access to it.

If you want more control over where the user's home directory resides within a share point or what it is named, click the Add (+) or Duplicate (copy icon) button to create a custom home directory. See "Creating a Custom Home Directory" (next) for instructions.

Creating a Custom Home Directory

In Workgroup Manager, you can customize a user's home directory settings. You'll want to customize home directory settings when:

- You want the user's home directory to reside in directories not immediately below the home directory share point. For example, you may want to organize home directories into several subdirectories within a share point. If Homes is the home directory share point, you may want to place teacher home directories in Homes/Teachers and student home directories in Homes/Students.
- You want to specify a home directory name different from the user's first short name.

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

You can also use Workgroup Manager to review home directory information in any accessible read-only directory domain.

To create a custom home directory using Workgroup Manager:

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

The share point for a local user account's home directory should reside in an AFP share point on the server where the user's accounts resides. This share point does not have to be automountable (it does not require a network mount record).

The share point for the home directory of a user account in a shared directory domain can reside in any AFP or NFS share point that the user's computer can access. The share point must be automountable—it must have a network mount record in the directory.

See "Setting Up an Automountable AFP Share Point for Home Directories" on page 110 or "Setting Up an Automountable NFS Share Point for Home Directories" on page 111 for instructions.

2 If you want the home directory to reside beneath a folder under the share point, use the Finder to create all the folders in the path between the share point and where the home directory 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 small globe above the accounts list and open the directory domain where the user account is stored. Click the Users button and select the user.

4 To be authenticated, click the lock.

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

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

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

7 In the URL field, either enter the full URL to an existing automountable AFP share point where you want the home directory 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 directory with the server's IP address: AFP://192.168.2.1/Homes." You can use or omit a slash (/) at the end of the URL.

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

For example, you might enter "Teachers/SecondGrade/Smith."

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 directory, concluding with the home directory itself.

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

Example for a local user account: /Users/Teachers/SecondGrade/Smith

Example for a user account in a shared directory domain:
/Network/Servers/myServer/Homes/Teachers/SecondGrade/Smith

The name you type following "/Network/Servers/" must be the host name entered when the server was initially set up. If you do not know the host name, open the Terminal application, type "hostname" and press Return to display the name.

10 Click OK.

11 (Optional) Enter a disk quota and specify megabytes (MB) or gigabytes (GB).

12 Click Create Home Now, then click Save.

The home directory has the name specified in step 8.

If you do not click Create Home Now before clicking Save, the home directory is created the next time the user restarts the client computer and logs in remotely.

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

13 For a user account in a shared directory domain, make sure that the user restarts his or her client computer so that the share point is visible on it.

Setting Up an Automountable AFP Share Point for Home Directories

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

Home directories 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—it must have a network mount record in the directory domain where the user account resides.

An automountable share point ensures that the home directory is visible in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain. It also lets other users access the home directory using the ~*home-directory-name* shortcut.

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

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

  Because of the way home directory disk quotas work, you may want to set up home directory share points on a partition different from other share points. See "Setting Disk Quotas" on page 113 for more information.

2 In Workgroup Manager, connect with the server in step 1 and click Sharing.

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 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.

6 Set Owner privileges to Read & Write, set Group privileges and Everyone privileges to Read Only, and click Save.

7 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 in which the user account resides. Then click the lock and authenticate as an administrator of the directory domain.

8 Select "Create a mount record for this share point" and "Use For User Home Directories."

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

10 Set up guest access to the share point so that users with home directories on different servers can access the home directory using the ~*home-directory-name*/Public shortcut.

  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. (They are selected by default.)

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

Setting Up an Automountable NFS Share Point for Home Directories

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

An automountable share point ensures that the home directory is visible in /Network/Servers automatically when the user logs in to a Mac OS X computer configured to access the shared domain. It also lets other users access the home directory using the ~*home-directory-name* shortcut.

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

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

Because of the way home directory disk quotas work, you may want to set up home directory share points on a partition different from other share points. See "Setting Disk Quotas" on page 113 for more information.

2 In Workgroup Manager, connect with the server in step 1 and click Sharing.

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

4 Click General and select "Share this item and its contents."

5 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.

6 Set Owner privileges to Read & Write, set Group privileges and Everyone privileges to Read Only, and click Save.

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

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

9 Add client computers 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 the Computer list.

Click Remove to remove the selected address from the list.

10 Set up share point privileges.

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

11 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 in which the user account resides. Then click the lock and authenticate as an administrator of the directory domain.

12 Select "Create a mount record for this share point" and "Use For User Home Directories."

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

Setting Disk Quotas

You can limit the disk space a user can consume to store files he or she owns in the partition where his or her home directory resides.

This quota doesn't apply to the home directory share point or to the home directory, but to the entire partition within which the home directory share point and the home directory reside. Therefore, when a user places files into another user's folder, it can have implications on the user's disk quota:

- When you copy a file to a user's AFP drop box, the owner of the drop box becomes the owner of the file.
- In NFS, however, when you copy a file to another folder, you remain the owner and the copy operation decrements *your* disk quota on a particular partition.

To set up a home directory share point disk quota using Workgroup Manager:

1 In Workgroup Manager, 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 small globe above the accounts list and open the directory domain where the user account is stored, click the Users button, and select the user.

3 To be authenticated, click the lock.

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 on which the share point resides.

Click Sharing, select the volume in the All list, and choose "Enable disk quotas on this volume."

Defining Default Home Directories by Using Presets

You can define default home directory settings to use for new users by using a preset to predefine them. See "Using Presets to Create New Accounts" on page 59 for information about defining and using presets.

Moving Home Directories

If you need to move a home directory, create the new one and manually delete the existing one to deallocate disk space it uses if you no longer need the existing one.

Deleting Home Directories

When you delete a user account, the associated home directory is not automatically deleted. You must delete it manually.

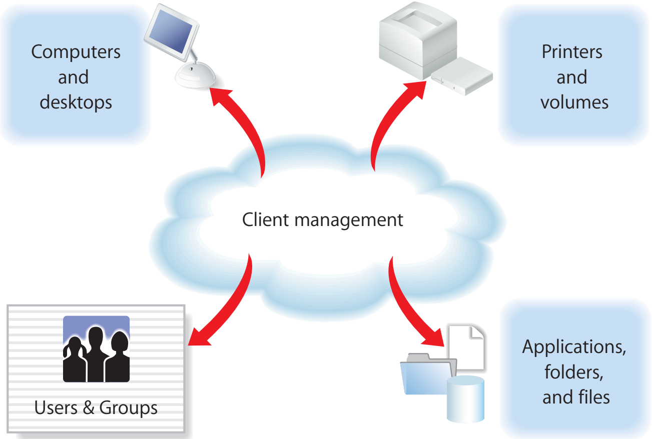
Client Management Overview

8

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 directories, group directories, 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 booting 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.

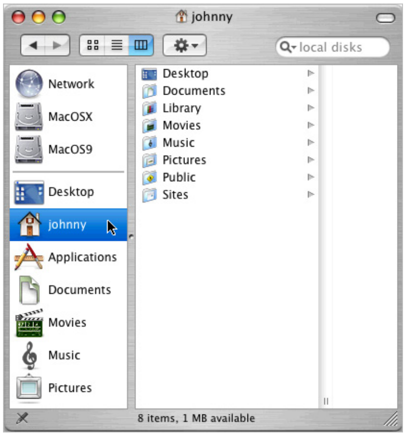
Using Network-Visible Resources

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.

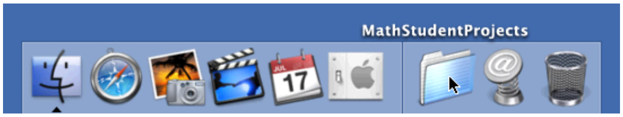
- **Network home directories**. A *home directory,* often referred to as a *home folder* or simply *home,* is a place for each Mac OS X user to keep personal files. Users with records in a shared Open Directory directory may have home directories that reside on the network, often on the same server where the user account resides.

  A home directory contains several folders—such as Desktop, Documents, and Public—to help organize information. After logging in, a user accesses his or her network home directory 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 easy network access wherever a user wants to work on group activities.



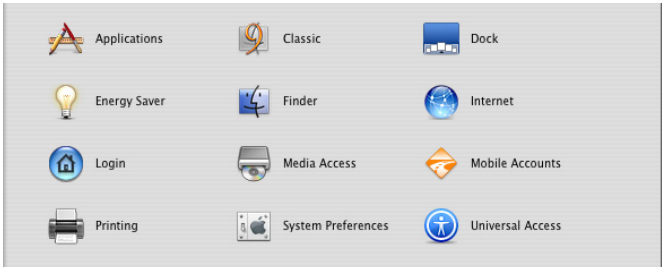
- **Other shared folders.** You can set up other folders on the server to provide network user access to applications, handouts, announcements, schedules, and other information.
- **Boot and install images.** You can use boot images and install images located on the server to automate the setup of network users' computers.

  A user's computer can start up from a *boot 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.

  An *install image* automatically installs software on users' computers, making it easy to deploy the operating system, additional applications, and even custom computer settings remotely and without user interactions.

Defining Preferences

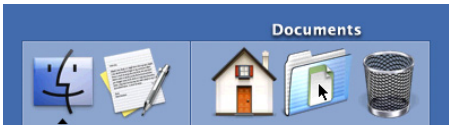
You manage a network user's work environments by defining preferences, settings that customize and control a user's computer experience.



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 allowable. 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 implement system capabilities that best reflect your user and business requirements.

The Power of Preferences

Many preferences, such as Dock and Finder preferences, are used to customize the appearance of desktops. 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:

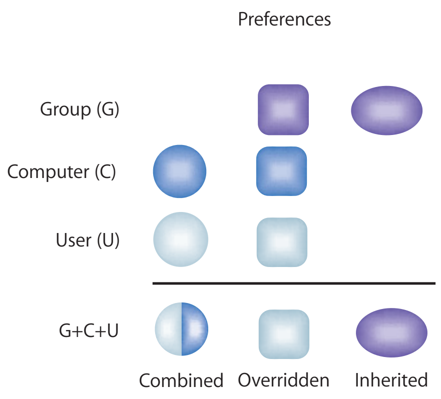
This preference	Tailors the work environment	Limits access and control	By letting you manage
Applications		x	The applications a user can open
Classic	x		Classic environment startup
Dock	x		The appearance and contents of the Dock
Energy Saver	x		Computer wake, sleep, startup, and shutdown settings
Finder	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
Mobile Accounts	x		The creation of mobile accounts
Printing		x	Which printers a user can use
System Preferences		x	Which system preferences are visible on the user's computer
Universal Access	x		Hardware settings for users with special visual, auditory, or other needs

Levels of Control

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 associated with it 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 can be defined only for computer lists, but other preferences can be set for user, workgroup, and/or computer lists.

The illustration below shows how managed preferences interact when the same preferences are set at multiple levels:



- Printing, Applications, and some Dock preferences (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.

- Other preference settings defined at more than one level may be **overridden** at login. When a user logs in to a managed computer and chooses a workgroup, user preferences override redundant computer preferences, and computer preferences override redundant workgroup preferences.

  For example, you may 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.

Suppose you select Left as the Dock's position on the screen for Workgroup A, but you select Bottom for the Dock position for the computer list containing Computer 2, and you select Right as the Dock position for user Alice. When Alice logs in to Computer 2 and chooses Workgroup A, the Dock will be on the right side of her screen.

Now suppose that you decide to stop managing the Dock Display settings for Alice (you select Not Managed in Alice's Dock Display preferences pane). When Alice logs in to Computer 2 and chooses Workgroup A, the Dock will be on the bottom of her screen.

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 occur, and the user inherits them 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.

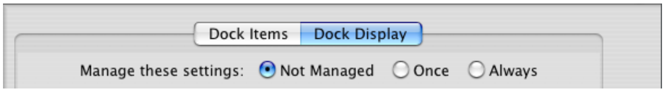
  For example, a student may belong to a group called "Class of 2011" for administrative purposes and to a workgroup called "Students" to limit application choices and provide a group shared folder for turning in homework. Another workgroup may be "Teacher Prep," used to provide faculty members access 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 after login take effect. More about managing the login experience appears next.

Degrees of Permanence

When you define preferences, you can choose to manage them Always or Once; they are Not Managed by default.



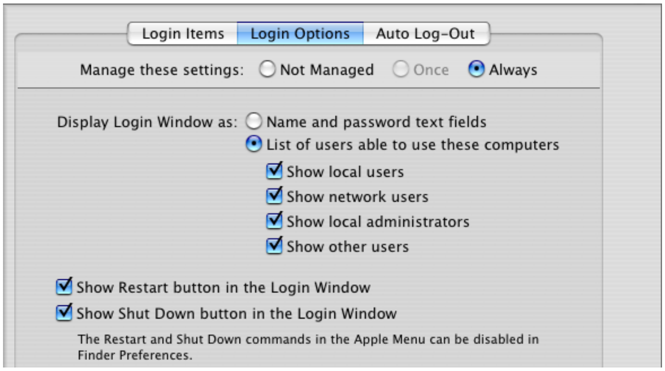
Manage these settings: ● Not Managed ○ Once ○ Always

- *Always* causes the preferences to remain in effect until you change them on the server. You can use the Always setting, for example, to make sure users can't add or remove Dock items.
- *Once* is available for some preferences. It's a quick and easy way to set up default preferences without managing them. 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.

  You can't set the following preferences to Once: Applications, Finder (Commands), Mobile Accounts, Printing, System Preferences, Login (Login Options and Auto Log-Out), and Energy Saver. For these preferences you must choose either Always or Not Managed.
- *Not Managed* 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.

Designing the Login Experience

You can set up Login preferences for computer lists to control the appearance of the login window. For example, these login options



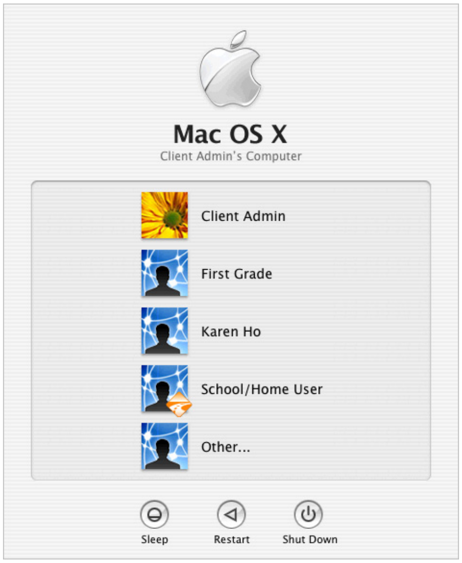
Manage these settings: ○ Not Managed ○ Once ● Always

Display Login Window as: ○ Name and password text fields
● List of users able to use these computers
☑ Show local users
☑ Show network users
☑ Show local administrators
☑ Show other users

☑ Show Restart button in the Login Window
☑ Show Shut Down button in the Login Window

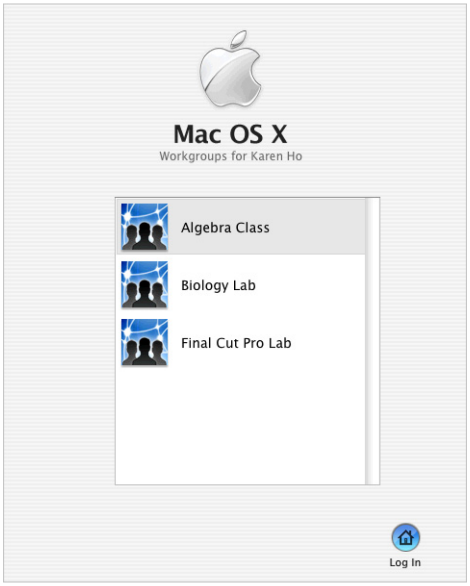
The Restart and Shut Down commands in the Apple Menu can be disabled in Finder Preferences.

result in a login window that looks like this:



The first user 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.

To log in, a user selects his or her login name in the list, then types a password when prompted. If the user belongs to more than one workgroup, a list of workgroups appears so the user can select the environment of interest. Note that it's possible for a user to belong to a group that doesn't appear in the list; only workgroups (groups with managed preferences) are listed.



Mac OS X
Workgroups for Karen Ho

- Algebra Class
- Biology Lab
- Final Cut Pro Lab

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.

Caching Preferences

Preferences are 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 also 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.

Helping Users Find Applications

Applications can be stored locally on a user 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.

To make specific local 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 a user is permitted to open.

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 132. Whether you choose to use the Simple Finder or the Regular Finder user environment, this list of approved applications determines what users find in the My Applications folder located in the Dock.

For more information about using the Simple Finder or Regular Finder, see "Hiding the Alert Message When a User Empties the Trash" on page 149. To place an alias to My Applications and other folders in a user's Dock, see "Adding Items to a User's Dock" on page 141.

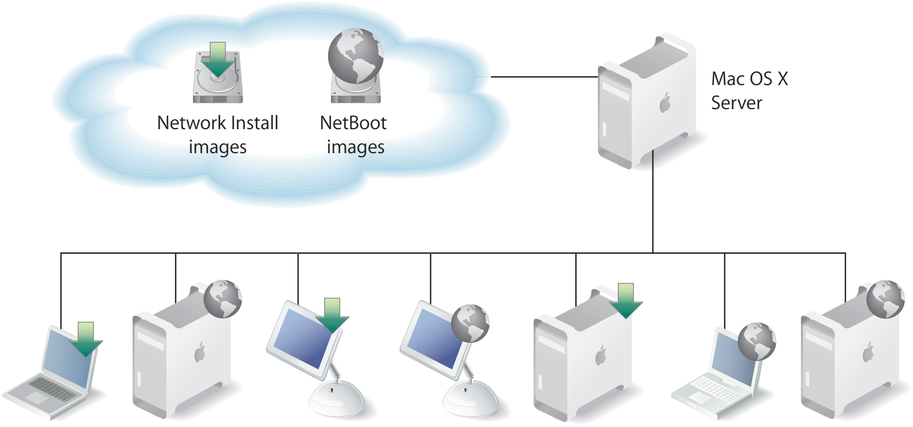
Helping Users Find Group Folders

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.

You use the Dock Items preference. To learn more, read "Providing Easy Access to Group Folders" on page 141. To provide access to the group volume, which contains the Public Folder and Drop Box for the group, see "Providing Easy Access to the Group Share Point" on page 158.

Installing and Booting Over the Network

The key to fast initial setup of multiple user computers and rapid refresh of computers is the use of Network Install and NetBoot images that reside on Mac OS X Server. User's computers start up using those images automatically.



You use Network Install images when you want to install software on user computers. You use NetBoot images when you want users' computer environments to be refreshed every time their computers are started.

Using a network-based boot image provides many advantages over booting from a local hard drive:

- The NetBoot image is locked from the user perspective. It can't be accidentally or maliciously damaged. In a training lab where students may make mistakes or in a computer science class where system protection can't be used because of programming tool needs, a NetBoot image allows computers to be restarted to their original state after each use. No matter what a student does while on the system, the image snaps back 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 boot 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 be used to provide a single image for optimum throughput.

  The 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 particular users, and another image can be used for booting computers in particular classrooms, offices, or labs.

Day-to-Day Client Administration

Administering networked computers entails recordkeeping, help desk operations, and minor updates while users are logged in and working. To accomplish these and other day-to-day tasks, you can use Apple Remote Desktop (ARD). ARD provides a remote management environment that simplifies user computer setup, monitoring, and maintenance:

- **Screen observation.** View user compvuter screens on your computer to monitor activities.
- **Screen control.** Show users how to perform tasks by controlling their screens from your computer.
- **Screen sharing.** Display your screen or a user's screen on user computers for training and demonstration purposes.
- **Screen locking.** Prevent users from using their computers.
- **Text communications.** Exchange messages with one or more users, and host questions and requests from individual users.
- **Hardware and software management.** Audit hardware information and software installed. Search for specific files and folders on user systems.
- **Software distribution and startup.** Identify NetBoot or Network Install images for user computers to use. Initiate network installations and user computer shutdown and startup. Use ARD 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

9

This chapter provides information about managing preferences for users, workgroups, and computers.

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 settings unmanaged).

Important: To manage Mac OS 9 clients, read Chapter 10, "Using Macintosh Manager for Mac OS 9."

In addition to various settings for users, groups, and computer lists, Workgroup Manager provides control over these preferences:

Preference pane	What you can manage
Applications	Applications available to users
Classic	Classic startup settings, sleep settings, and the availability of Classic items such as Control Panels
Dock	Dock location, behavior, and items
Energy Saver	Battery usage for portable computers, and sleep or wake options.
Finder	Finder behavior, desktop appearance and items, and availability of Finder menu commands
Internet	Email account preferences and web browser preferences
Login	Login window appearance, mounted volumes, and items that open automatically when a user logs in
Media Access	Settings for CDs, DVDs, and recordable discs, plus settings for internal and external disks such as hard drives or floppy disks
Mobile Accounts	Creation of mobile account at login
Printing	Available printers and printer access

Preference pane	What you can manage
System Preferences	System preferences available to users
Universal Access	Settings to control mouse and keyboard behavior, enhance display settings, and adjust sound or speech for users with special needs

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. Group preferences are stored on the group volume. User preferences are stored in the user's home directory (the Home folder on Mac OS X clients).

After user 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 or a local home directory. For information about how to set up a group volume or how to set up home directories for users, see Chapter 4, "Setting Up User Accounts."

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. 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 Open Directory to indicate that change. When a user logs in, the client updates any flagged accounts automatically. If you manage directory services using a different tool, you can still use Workgroup Manager to update the cache at fixed intervals.

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.

Updating the Managed Preferences Cache at Intervals

You can update a user's managed preference cache regularly. This setting applies only to computer lists. The computer checks the server for updated preferences according to the schedule you set.

To set an update interval for the managed preferences cache:

1. In Workgroup Manager, click Accounts.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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, 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.

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 empty the managed preferences cache:

1. In Workgroup Manager, click Accounts.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
3. Click the Computer Lists button and select one or more computer lists.
4. Click Cache, then click "Update Cache."

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), then click Refresh Preferences in the dialog displayed.

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 Not Managed or Once.

To manage user preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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, choose a management setting.

   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.

Note: A user can access only 16 workgroups at a time, so plan accordingly.

To manage group preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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, choose a management setting.

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Click the Computer Lists button and select one or more computer lists.

4 Click the icon for the preference you want to manage.

5 In each preference pane, choose a management setting.

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 will have the new setting you choose. For example, suppose you select three group accounts that each have different settings for the Dock size. When you look at the Dock Display preference pane for these accounts, the Dock Size slider is centered and has a dash on it. If you change the position of the Dock Size slider to Large, all selected accounts will have a large-size Dock.

Disabling Management for Specific Preferences

After you set up managed preferences for any account, you can turn off management for specific preference panes by setting the management setting to Not Managed.

To selectively disable preference management:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click the icon for a preference that is currently being managed.

5 Click a button to display the pane containing the preference settings you no longer want to manage.

In some cases (Printing and Media Access, for example), you can skip this step because the management settings apply to all panes in the preference.

6 Select Not Managed.

7 Click Apply Now.

When you change the preference management settings, the new setting applies to all items in the active preference pane. If you want to disable all management for an individual preference (for example, Dock), make sure the management setting is set to Not Managed 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 users are allowed to open, and you can allow users to open items on local volumes.

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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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.

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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 allow this option.

To allow access to UNIX tools:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 table below describes what settings on 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 after 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 document that requires such an application. You can also choose to display an alert when Classic starts and give users the option of cancelling Classic startup.

To work with various startup options for Classic:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 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 will start up automatically when a user opens a document or an application that requires it. In this case, the Classic startup window will be 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 will be 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 situation, 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 will see an error message and be 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 System preference.

To choose a specific Classic System Folder:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Classic.

5 Click Startup.

6 Set the management setting to Always.

7 Type 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 System preference, 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 or rebuilding the Classic desktop file, when they start or restart Classic from the Advanced pane of the Classic System preference. You may want to allow this privilege 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 the Classic System Preference.

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. See "Managing Access to Applications" on page 132 for more information.

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 vs. non-PostScript printers).

To hide or show items in the Apple menu:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 will go to sleep to reduce its use of system resources. You can adjust the amount of time Classic waits before going to sleep after a user quits the last Classic application. If Classic is in sleep mode, opening a Classic application may take a little longer.

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 will suspend 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 will be 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 per 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 settings on each Dock pane can do.

Dock preference pane	What you can control
Display	The Dock's position and behavior
Dock Items	Items and their position in a user's Dock

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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, then adjust the slider. Magnification is useful if you have many items in the Dock.

9 If you don't want the Dock to be visible all the time, select "Automatically hide and show the Dock." When the user moves the pointer to the edge of the screen where the Dock is located, the Dock pops up automatically.

10 Select whether to place the Dock on the left, right, or bottom of the desktop.

11 Select a minimizing effect.

12 If you don't want to use animated icons in the Dock when an application opens, deselect "Animate opening applications."

13 Click Apply Now.

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 "Working With Group Folder Settings" 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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).

7 To add individual applications, regular folders, and documents to the Dock, click Add to browse and select the item you want.

To remove a Dock item, select it and click Remove.

You can rearrange Dock items in the list by dragging them into the order in which you want them to appear. Applications are always grouped at one end; folders and files are grouped at the other.

8 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 available applications.

The Documents folder is the Documents folder found in the user's home directory.

The Network Home folder is primarily for mobile accounts. It is the user's home directory that is housed on the server.

9 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Dock.

5 Click Dock Items, then set the management setting to Always.

6 Deselect "Users may add and remove additional Dock items."

7 Click Apply Now.

Managing 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. The table below summarizes what you can control with the settings on each Energy Saver pane.

Energy Saver preference pane	What you can control
Desktop	Sleep timing for the computer's hard drive and display
Portable	Processor performance settings in addition to sleep, wake, and automatic restart responses for portable computers
Battery Menu	Whether the battery status indicator appears for users
Schedule	Regular schedules for startup, shutdown, or sleep

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 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 computer waits to enter sleep mode. The default setting is 1 hour. The computer will 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 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, users 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 computer waits to enter sleep mode. The default setting is 1 hour. The computer will 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."

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 as either a direct or backup power source when not connected to a power adapter. When battery power is too low to function, the computer will put itself to sleep to conserve energy. When a user reconnects the computer to a direct power source (such as by inserting a fresh battery or connecting a power adapter), they 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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. 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 or not 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 directory of the computer.

Setting Up Simple Finder

You can select either the regular Finder or Simple Finder as the user environment. The regular Finder looks and acts like the standard Mac OS X desktop. Simple Finder provides an easier-to-navigate interface (for example, the Documents and My Applications folders appear in the user's Dock).

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 Simplified 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 Simplified 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 (directory). These users can't use applications because Simple Finder prevents access to the group directory.

To turn on Simple Finder:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 If you select Always, you can select either "Use normal Finder" or "Use Simplified Finder to limit access to this computer."

If you select Once, only "Use normal Finder" is available.

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 directory 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 what directory appears when a user opens a new Finder window. You can also define how contents are displayed when a user opens folders.

To set Finder window preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 directory.

Select Computer to show the top-level directory, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 using the "Connect to Server" command in the Finder's Go menu and providing the server's name or IP address. If you don't want users to have this menu item, you can hide the command.

To hide the "Connect to Server" command:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 use the "Go to iDisk" command in the Finder's Go menu. If you don't want users to see this menu item, you can hide the command.

To hide the "Go to iDisk" command:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 privilege, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 will work only with CD-R, CD-RW, or DVD-R disks. Only a SuperDrive can burn DVDs.

Controlling User Access to Folders

Users can open a specific folder by using the "Go to Folder" command in the Finder's Go menu and providing the folder's path name. If you don't want users to have this privilege, you can hide the command.

To hide the "Go to Folder" command:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 computers 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 155.

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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Views, 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 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 or not to show the toolbar in a Finder window.

Default View settings control the overall appearance of all Finder windows. Computer View settings control the view for the top-level computer directory, showing hard disks and disk partitions, external hard disks, mounted volumes, and removable media (such as CDs or floppy disks).

To set preferences for the default and computer views:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Finder.

5 Click Views, 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 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," then choose a method from the arrangement pop-up menu. You can arrange items by name, creation or modification date, size, or kind (for example, all folders grouped together).

9 Adjust List View settings for the default view.

If you select "Use relative dates," an item's creation or modification date is displayed as "Today" instead of "4/12/02," for example.

If you select "Calculate folder sizes," the computer calculates the total size of each folder shown in a Finder window. This can take some time if a folder is very large.

Select a size for icons in a list.

10 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 settings on 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 starting point 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 user login options, provide password hints, and control the user's ability to restart and shut down the computer from the login screen. You can also mount a group volume or make applications open automatically when a user logs in. The table below summarizes what you can do with the settings on each Login pane.

Login preference pane	What you can control
Login Items	Access to the group volume, which applications open automatically for the user
Login Options	For computer lists only: The appearance and function of items in the Login window, Fast User Switching
Auto Logout	For computer lists only: How many minutes of inactivity result in the user being logged out

Login Options and Auto Logout 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 will see 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Login.

5 Click Login Options 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 a type of user doesn't show up in the list, deselect the corresponding setting. If you allow unknown users, you can select "Show other users."

Note: When the "Allow users with local-only accounts" checkbox is deselected (in Workgroup Manager/Accounts/Computer Lists/Access), local non-administrators won't be able to log in.

8 You may want to allow some users (for example, administrators) to log in using a Darwin console (command-line interface). To enable this option, select "Allow users to log in using '>console.'"

9 To automatically log in as a specific user when the computer starts up, you can select Enable Auto Login Client Setting. This setting can be useful if you want to set up a generic public use computer or a kiosk.

If you use this setting, you must set up automatic login on the client computer. Open System Preferences, click Accounts, click Login Options, select "Automatically log in as," 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 an automatically opened item, 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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 privilege. (This checkbox is available only if Login Items preferences are always managed.)

   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. Click Apply Now.

Providing Access to a User's Network Home Directory

This setting is used primarily for mobile accounts. When a user logs in while connected to the network, the share point with the user's original home directory (located on the server) is mounted on the desktop.

To automatically mount the Network Home:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 directories by accessing the share point automatically at login. (For information about setting up a group share point, see "Working With Group Folder Settings" 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 in the list under "Open these items automatically when the user logs in."

If you don't want the group share point to appear in the Dock, select the Hide checkbox.

10 Make sure the "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 will 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 147.) Check the Commands pane of Finder preferences and make sure Restart and Shut Down are not selected.

Note: Login Options 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Click the Computer Lists button and select one or more accounts.

4 Click Login.

5 Click Login Options and set the management setting to Always.

6 Deselect the "Show Restart" and "Show Shut Down" buttons.

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.

Note: Login Options settings are available only for computer lists.

To show a password hint:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Click the Computer Lists button and select one or more accounts.

4 Click Login.

5 Click Login Options and set the management setting to Always.

6 Select "Show password hint after 3 attempts to enter a password."

7 Click Apply Now.

Allowing Simultaneous Multiple 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 selecting 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 manage Fast User Switching:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Click the Computer Lists button and select one or more accounts.

4 Click Login.

5 Click Login 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 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 10.3 and later.

To log a user out automatically:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Click the Computer Lists button and select one or more accounts.

4 Click Login.

5 Click Auto Log-Out and set the management setting to Always.

6 Adjust the slider to set the amount of time a user can remain inactive before automatic logout occurs.

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 on 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 to use CDs, DVDs, or recordable discs 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": 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 or save files on it.
7. Click Apply Now.

Ejecting Items Automatically When a User Logs Out

On computers used by more than one person, such as in a computer lab, users may sometimes forget to take their personal media with them when they leave. If they don't eject disks, CDs, or DVDs when they log out, these items may be available to the next user who logs in.

If you allow users to access CDs, DVDs, or external disks such as Zip disks or FireWire drives on shared computers, you may want to automatically eject removable media when a user logs out.

To eject removable media automatically:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
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 Mobile Accounts Preferences

If a user requires a mobile account, you can create one for the user automatically during login. For more details about mobile accounts, including how to use the Mobile Accounts preference setting, see Chapter 3, "User Management for Mobile Clients."

Managing Printing Preferences

Use Printing preferences to create printer lists and manage access to printers. The table below describes what settings on 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 final list of printers is a combination of printers available to the user, the group selected at login, and the computer being used.

To create a printer list for users:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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, 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 (adding or removing printers).

To restrict access to the printer list:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 computers. For example, if you have a computer in a classroom with a printer attached, you can reserve that printer for teachers only by making the teacher an administrator and requiring an administrator's user name and password to access the printer.

To restrict access to a printer connected to a specific computer:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 don't want users to access local printers, deselect "Allow printers that connect directly to the user's computer." To require an administrator password 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 printer dialog.

To set the default printer:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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, then select "Require an administrator password."

8 Click Apply Now.

Managing Access to System Preferences

You can specify which System Preferences are visible to users and which preferences users can modify. Users can open any item that appears in System Preferences but they may not be able to change its settings. Some preferences, such as Startup Disk preferences, always require an administrator name and password.

The preferences that appear in Workgroup Manager are those installed on the computer you're currently using. If your administrator computer is missing any System Preferences, you should either install them or use Workgroup Manager on an administrator computer that has those preferences installed.

To manage access to System Preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

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 special needs.

The table below describes what settings on 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 or not 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 right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
3. Select one or more users, groups, or computer lists.
4. Click Universal Access.
5. Click Seeing, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Hearing, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Keyboard, 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 for 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 goes.

To control mouse and pointer settings:

1 In Workgroup Manager, click Preferences.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Mouse, 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 right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select one or more users, groups, or computer lists.

4 Click Universal Access.

5 Click Options, 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

If necessary, you can allow managed users to use assistive devices, such as a text reader.

To allow assistive devices:

1. In Workgroup Manager, click Preferences.
2. Make sure the right directory is selected and that you are authenticated for it.

   To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.
3. Select one or more users, groups, or computer lists.
4. Click Universal Access.
5. Click Options, then select the Always management setting.
6. Select "Enable access for assistive devices."
7. Click Apply Now.

Using Macintosh Manager for Mac OS 9

10

This chapter describes how to provide network administrators with a way of managing Mac OS 9 client computers, controlling access to software and removable media, and providing a personalized experience for users.

About Macintosh Manager

Macintosh Manager provides network administrators with a centralized method of managing Mac OS 9 client computers, controlling access to software and removable media, and providing a consistent, personalized experience for users. After you import basic information (user name, password, and user ID) from Workgroup Manager user accounts, you can customize preferences and privileges for users, workgroups, and computer lists. Mac OS X Server saves user documents and preferences in a home directory, so your users can access their files from any Mac on your network.

Like Workgroup Manager, Macintosh Manager lets you set network-wide policies for controlling user access to applications, file server volumes, and printers. Macintosh Manager provides its own authentication and preference management for Mac OS 9 computers and can be used with NetBoot clients.

Client management can help you create a more tailored and efficient user experience. Because you can define the user environment, you can provide an interface suitable for users with different skill levels. This can make it easier, for example, to set up an elementary school computer lab for use by a wide range of students from kindergarten to eighth grade.

This chapter summarizes how Macintosh Manager works, gives details about different types of managed environments, and tells you how to:

- Set up Macintosh Manager.
- Import users into Macintosh Manager.
- Set up workgroups and computer lists for Mac OS 9 clients.
- Create managed environments for Mac OS 9 clients.
- Implement Macintosh Manager security settings and controls.

Note: Macintosh Manager is not used to manage Mac OS X clients. If you need to manage Mac OS X clients, read Chapter 9, "Managing Preferences."

Transition Strategies for Macintosh Manager

If you're migrating to Macintosh Manager 2.2.2 from an earlier version, you can do a simple upgrade to the new Macintosh Manager. Functionality remains much the same, but you may notice some differences in how Macintosh Manager stores certain items.

If you need more information about migration issues and strategies, refer to the migration guide.

The User Experience

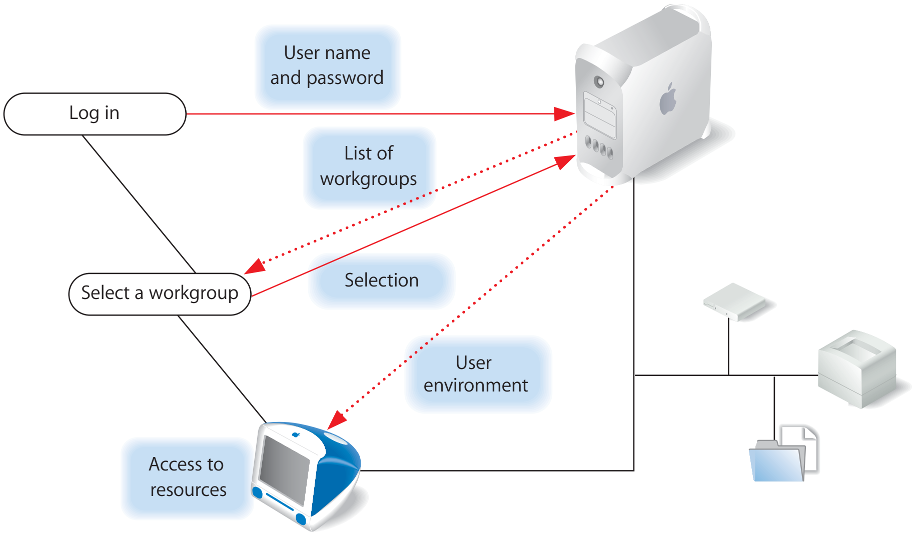
This section describes both the actual user experience and the server processes for Mac OS 9 managed clients.

Logging In

On Mac OS 9 client computers, users that have been imported into Macintosh Manager can simply type their Mac OS X Server user names and passwords in the Macintosh Manager login dialog. Alternatively, you can allow users to choose their names from a list (showing long names) at login.

When a user logs in, Macintosh Manager uses Directory Services to verify that the user ID is valid. If it is valid, Macintosh Manager finds the correct workgroups for that user and displays them in a list. If a user belongs to more than one workgroup, he or she can select a workgroup from the list. If a user belongs to only one workgroup, login proceeds automatically without displaying a workgroup list. Macintosh Manager workgroup settings define the user's working environment (Finder, Restricted Finder, or Panels). Note that if the server that contains information about the user's name and password is unavailable, that user will not be able to log in.

Depending upon the computer being used, the network configuration, and access privileges, the user may have access to various resources such as printers, applications, and volumes. Settings for the computer, the workgroup, and the user determine the final set of privileges and preferences that define the user experience for an individual.



Logging In Using the All Other Users Account

Users who have a Mac OS X user account but haven't been imported into Macintosh Manager can type their Mac OS X Server user names and passwords in the Macintosh Manager login dialog. If the All Other Users account belongs to more than one workgroup, the user can select a workgroup from a list. Otherwise, login continues automatically.

Logging In Using the Guest Account

Any user can log in as Guest, provided that the Guest account has been activated. The Guest account doesn't require password authentication. If the Guest account belongs to more than one workgroup, the user can select a workgroup from a list. Otherwise, login continues automatically.

Locating the Home Directory

User home directories are mounted automatically when a user logs in. A folder with the user's name on it appears on the desktop or on a panel depending upon the workgroup type. The user's home directory is located inside the Users folder. In mixed environments, this may be the same home directory used by Mac OS X.

Guest users have a temporary local home directory for storing files or preferences.

Finding Applications

Approved applications for Panels and Restricted Finder workgroups are located in the "Items for *workgroup name*" folder inside the user's home directory. For users in a Finder workgroup, applications are stored in the client computer's Applications folder or Applications (Mac OS 9) folder.

Finding Shared Documents

Depending on the user environment and how you set up workgroup folders, users may have access to areas where they can view or store shared items. For example, you can create a hand-in folder for a Panels workgroup to allow users to turn in documents or enable collaboration by creating a group documents volume in the Macintosh Manager share point.

Before You Begin

You should consider taking advantage of client management if:

- You want to provide users with a consistent, controlled interface while allowing them to access their documents from any computer
- You want to control privileges for users with portable computers
- You want to reserve certain resources for only specific groups or individuals
- You need to secure computer usage in areas such as administrative offices or open labs

Before you set up Macintosh Manager to manage users, groups, or computers, be sure to follow these preliminary steps.

Step 1: Make sure computers meet minimum requirements

Important: If you have clients using earlier versions of Macintosh Manager, be sure to upgrade them to Macintosh Manager 2.2.2 before you connect them to the Mac OS X Server.

Client Computer Requirements

Software

- Mac OS 9.x as the primary operating system
- Appearance control panel v. 1.0.1 or later

Note: Macintosh Manager is not used to manage Mac OS X clients, although user lists and home directories may be the same for Mac OS 9 and Mac OS X clients.

Hardware

- Macintosh computer with a 68K processor
- 8 megabytes (MB) of physical random access memory (RAM) (not virtual memory)
- 2 MB of disk space available
- 16-bit monitor recommended if using the Panels environment

Administrator Computer Requirements

Software

- Mac OS X Server (with Macintosh Manager administrator software) installed

  If you want to access the administrator software on a nonserver computer, you can also install only the Macintosh Manager administrator software (the computer must use either Mac OS X version 10.3 or Mac OS 9.2 as the operating system).

Hardware

- Macintosh computer with a G3 processor
- 128 MB of RAM; at least 256 MB of RAM for high-demand servers running multiple services
- 4 gigabytes (GB) of available disk space
- Minimum monitor resolution of 800 x 600

Note: Automatic hardware restart requires a Macintosh Server G4 or Power Mac G4 released in February 2000 or later.

Step 2: Install Macintosh Manager administrator software

You can use Macintosh Manager administrator software in either Mac OS X or Mac OS 9. You can install the administrator software on a Mac OS X server, on selected "administrative" client computers, or on all client computers. Only server administrators, Macintosh Manager administrators, and workgroup administrators have access to the Macintosh Manager administrator application.

Note: Macintosh Manager administrator software must be used remotely. You cannot use the Macintosh Manager software to administer Mac OS 9 clients from the same Mac OS X server you selected as your Macintosh Manager Server.

Using designated administrative computers can make it easier to change or update management settings for clients. For example, if you have a set of computers in a classroom, you could install the administrator software on the teacher's computer and give the teacher administrative access. Then, the teacher can make immediate changes as needed, such as adding users to a workgroup or providing access to a different printer.

Because the administrator computer is used to set up Macintosh Manager, the administrator computer should have access to the same printers and applications you want to use for your client computers. This makes it easier to create lists of allowed applications and printer lists for the clients. The administrator computer can have access to more printers and applications than clients but shouldn't have access to fewer.

Important: When you make printers available to client computers, Macintosh Manager creates desktop printers for your Mac OS 9 clients. The Mac OS X version of the Macintosh Manager administrator application only creates LaserWriter desktop printers. If you need to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients.

To set up an administrator client computer:

1 Make sure the computer meets minimum requirements.

2 Make sure the system software is either Mac OS X or Mac OS 9.2.

3 Make sure necessary applications are installed.

4 Set up printer access using either Printer Setup Utility (for Mac OS X) or Desktop Printer Utility (for Mac OS 9).

5 Install Macintosh Manager administrator and client software.

Before you use the Macintosh Manager administrator application, open the Sharing pane of System Preferences in Mac OS X and make sure web sharing and file sharing are turned off. If you're using Mac OS 9, check the settings for the File Sharing and Web Sharing control panels.

Step 3: Set up client computers

Only Mac OS 9 computers can be used as Macintosh Manager clients.

To set up Mac OS 9 client computers:

1 Make sure the computer meets minimum requirements.

2 Make sure the system software is Mac OS 9 (version 9.1 or later recommended).

3 Install Macintosh Manager client software, if it isn't already installed.

4 Open the Multiple Users control panel.

5 Click Options, then click Other.

6 Select "Macintosh Manager account (on network)."

7 Click Save.

8 Select On to turn on Multiple User Accounts.

9 Close the control panel, and then choose Logout from the Special menu.

The computer locates Macintosh Manager servers (any Mac OS X Server with Macintosh Manager server processes installed) on your network automatically when you log out. You can select the server you want to use. If the computer can't locate a Macintosh Manager server, browse to find the TCP/IP address (not the AppleTalk address) of the server you want.

Using Update Packages

If you're already using Macintosh Manager 2.0 or later on a client computer, you can easily upgrade to the latest version of Macintosh Manager by using an automatic update package. The update package is located on the Macintosh Manager installation CD. It is not installed automatically.

To use an update package:

- Copy the update package to the Multi-User Items folder on your Macintosh Manager server.

All connected clients periodically look for an update package in the Multi-User Items folder. If an update package is found, clients run the update automatically regardless of whether or not the update is for a new or previous version. Before you use an update package, be sure to shut down any computers you don't want to update. After the update is complete, remove the update package from the Multi-User Items folder, and then restart the client computers.

Choosing a Language for Macintosh Manager Servers and Clients

Ideally, the language used on client computers should match the language used on the Macintosh Manager server. However, if you want to set up different languages on certain client computers, you can do so.

Client computers using different languages can connect to the same server provided the server language script matches the client language script. For example, a user at a client computer that uses French-language client software with the script set to Roman can connect to the server. Another user at a German client computer using Roman script can also use the same server. You can set the script in the International pane of System Preferences (in Mac OS X) or using the International control panel (in Mac OS 9).

When a user connects to a Macintosh Manager server, the client computer should use the same language software that was used during any previous connections. For example, if a user connects to the Macintosh Manager server from a French client computer and then from a German client computer, preference folders and other folders in the user's home directory may be created for each language, so the user may not be able to share preferences across languages. On the other hand, if separate folders are not created, then different-language versions of two programs may end up sharing a preference file. This could cause the client computer to freeze.

Changing the Apple File Service Language Script

Before using a Macintosh Manager server, make sure the correct Apple file service language script (for "Encoding for older clients") is selected. If Macintosh Manager service is already in use, stop Macintosh Manager service before changing the language script. To change the language script, open Server Admin, select AFP, click Settings, and choose a script from the pop-up menu.

The “Encoding for older clients” script should match the client computer’s language script (selected in the International pane of System Preferences) in addition to the language script used for the Macintosh Manager administration application.

Step 4: **Make sure you’ve set up users and their home directories**
If you haven’t set up users and home directories, do so before you proceed. Read Chapter 4, “Setting Up User Accounts,” for more information.

Inside Macintosh Manager

The sections that follow describe some of Macintosh Manager’s components and provide background information about how Macintosh Manager works with other Mac OS X Server services.

Macintosh Manager Security

Although Macintosh Manager is not a designated “security application,” you can use Macintosh Manager settings to provide more administrative control or to allow greater flexibility for users. For example, you might want to restrict local file and system access privileges, allow users to play audio CDs, or allow users to access some applications but not others.

Macintosh Manager users cannot access other users’ home directories, nor can they change network settings (AppleTalk and TCP/IP control panels), Energy Saver settings, or Multiple Users settings.

Macintosh Manager’s design prevents users from renaming Macintosh Manager files or changing the file type or creator. In addition, the Multiple Users extension is not affected if a computer is restarted with extensions off, and users cannot disable the Multiple Users extension by moving it or turning it off.

About the Macintosh Manager Share Point

When Macintosh Manager server software is installed, a share point named Macintosh Manager is created on the server. Its permissions are automatically set to allow access from Macintosh Manager. Users who don’t have administrative privileges can’t see the contents of the share point and don’t interact with it. The Macintosh Manager share point exists primarily to service the databases, but it is also the default location for the workgroup document volume. Note that Macintosh Manager users count toward the number of connected users for File Server access licenses. For more information about the contents of the workgroup document volume, see “Sharing Information in Macintosh Manager” on page 205.

If you need to save space, you can move the Macintosh Manager share point to another volume as long as the name of the share point is the same, the folder remains a share point, and the access privileges are the same. Avoid using non-ASCII special characters (such as •, å, é, or ü) or any double-byte characters (such as Kanji characters) in the names of share points you plan to use with Macintosh Manager.

Important: Do not place the Macintosh Manager share point on a UFS-formatted volume.

Using Special Characters in Share-Point Names

Do not use non-ASCII special characters (such as •, å, é, or ü) or any double-byte characters (such as Kanji characters) in the names of share points you plan to use with Macintosh Manager.

The Multi-User Items Folder

The Multi-User Items folder is located in the Macintosh Manager share point. Files and folders inside the Multi-User Items folder contain information about options set using Macintosh Manager, such as the location of the Macintosh Management server, aliases to workgroup items, cache information, and the databases for users, groups, and computer lists. The Multi-User Items folder contains the following items:

- *Activity Log file:* This file contains log entries used to generate reports that show information such as login activity, printer usage, and application usage. You can define the number of entries in the Activity Log file. See "Setting the Number of Items in a Report" on page 225 for more information.
- *CD-ROM Preferences file:* This file contains a list of CDs users are allowed to use, along with any settings for specific items on each CD.
- *Computers folder:* This folder contains database files that store Macintosh Manager settings for each computer list you set up.
- *Groups folder:* This folder contains a folder for each Macintosh Manager workgroup and database files that store information about Macintosh Manager settings for each workgroup, such as the allowed items list and the location of the workgroup document folder.
- *Multi-User Items file:* This file contains an archive of the files currently inside the Multi-User Items folder. Don't open or modify the file. If it is deleted, it is created again the next time you use Macintosh Manager.
- *Printers folder:* This folder contains files that represent the desktop printers you set up in Macintosh Manager. A file is created for each desktop printer used by a Macintosh Manager workgroup. When a user logs in to a workgroup that uses a desktop printer, the printer information is copied to the desktop of the client computer.

  You should use Macintosh Manager to modify printer information; don't open or remove items in the Printers folder. If you delete a printer file from this folder, workgroup members who want to use that printer see a message that the printer can't be found.

- *Users folder:* This folder contains database files that store Macintosh Manager settings for each user account and a folder for each user that has logged in to the server at least once.

How the Multi-User Items Folder Is Updated

The client's Multi-User Items folder is always updated when you make changes in Macintosh Manager. A copy of this folder is stored automatically in the System Folder of each client computer. If the client computer's Multi-User Items folder is deleted, the computer downloads a new, clean copy from the server as needed, but not while a user is logged in. The folder is also updated under the following circumstances:

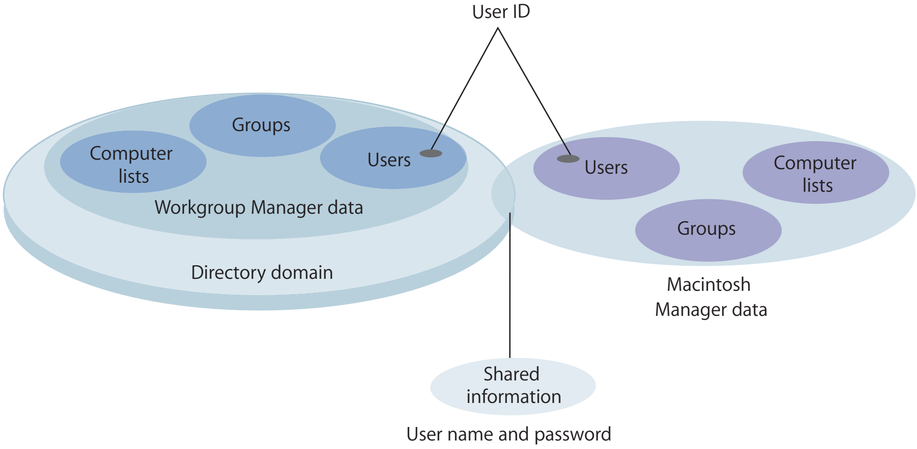
- If a client computer is connected to the server, but no users are logged in, Macintosh Manager checks periodically to see if any items in the folder need to be updated. If changes were made while a user is logged in to a computer, the folder isn't updated until the user logs out.
- If a computer is disconnected from the server automatically because it was idle for a period of time, no update checks are made until a user logs in and out of the computer.
- If the client's Multi-User Items folder is deleted, the client downloads a new, clean copy from the server when a user logs in.

How Macintosh Manager Works With Open Directory

Both Macintosh Manager and Workgroup Manager have access to user account information in a directory domain. If you're managing Mac OS 9 clients, you must import users from Workgroup Manager into Macintosh Manager or use Macintosh Manager's All Other Users feature in order to provide user access to your managed network.

The only information shared between Macintosh Manager and Workgroup Manager is the user ID, which is stored in a directory domain along with the user name, password, and information about the location of the user's home directory.

For more information about directory domains, see the Open Directory administration guide.



Macintosh Manager uses the user ID to verify and obtain a user's user name and password through Open Directory and to find the user's home directory. The user ID is also used to match users to the correct workgroups, preferences, and computer lists in Macintosh Manager.

All other user information, such as user storage quotas and system access privileges, is set up using Macintosh Manager. After users are imported, you can create workgroups for those users and create lists specifying which computers your workgroups can use. Macintosh Manager workgroups and computer lists are completely independent of Workgroup Manager groups and computer lists.

Where User Information Is Stored

Macintosh Manager stores information about settings for users, workgroups, and computers in database files located in folders inside the Multi-User Items folder. The Users, Groups, and Computers folders each contain two database files:

- One file contains an index of each record in the database (such as the name of a workgroup).
- The other file contains the specific information for each record (such as workgroup members, privileges, and environment).

Although the users, groups, and computers databases are not part of a larger relational database, each refers to information stored in the other databases. For example, the users database contains a list of workgroups to which a user belongs. To maintain consistency between databases, Macintosh Manager checks references from one database to another and updates the databases as needed.

How Macintosh Manager Works With Home Directories

You can set up home directory locations when you create user accounts. If a user doesn't have a home directory, he or she will not be able to log in (unless you select "Work offline if the user's home directory is not available"; to do so, click Computers, then click Security). Mac OS 9 managed clients mount the user's home directory automatically when a user logs in. The user is the owner of his or her own home directory and has full access to its contents. Macintosh Manager prevents access to other users' home directories, even if the folder's permissions have been set to allow access.

For more information about creating user accounts and home directories, see Chapter 4, "Setting Up User Accounts."

How Macintosh Manager Works With Preferences

In addition to controlling certain privileges, Macintosh Manager allows you to control application preferences and System Preferences. You can define these preferences using folders inside a user's Managed Preferences folder.

- Preferences in the Initial Preferences folder are set only once for a user.
- Preferences in the Forced Preferences folder are set every time a user logs in.

For more information about how to use these folders to control user preferences, see "Managing Preferences" on page 227.

Where Macintosh Manager Preferences Are Stored

This section describes how user-specific preferences (such as web browser "favorites" and desktop backgrounds) are stored in a Macintosh Manager environment.

Macintosh Manager stores and accesses preferences this way:

- *When a user is not logged in:* Most of a user's individual preferences are stored on the server, for both Mac OS 9 client computers.
- *When a user logs in to Macintosh Manager:* The individual preferences for that user are located by Macintosh Manager and put in effect for as long as the user is logged in. Mac OS 9 client preferences are stored in the /Library/Classic/Preferences folder in the user's home directory.

If a user doesn't have a home directory, you can store preferences for Mac OS 9 in the Preferences folder in the Users folder on the client hard disk, but you cannot store them in the Preferences folder in the System Folder.

Using the MMLocalPrefs Extension

If some applications create excess network activity, storing preferences locally may help decrease the overall burden on your network. You can install the MMLocalPrefs extension on Mac OS 9 computers to allow Macintosh Manager to store and access user preferences locally. Using the MMLocalPrefs extension may increase login and logout times because user preferences need to be copied to and from the local hard disk.

The MMLocalPrefs extension must be installed manually on individual computers, and it affects any user who can access those computers.

Important: Do not install the MMLocalPrefs extension if you need to enable the Check Out feature for Mac OS 9 clients.

Using NetBoot With Macintosh Manager

Although you're not required to use NetBoot for Mac OS 9 with Macintosh Manager, you can use it to administer each computer's system setup in labs and classrooms. With NetBoot for Mac OS 9, you can provide students with identical user environments and easy access to the same resources on a secure network that is easy to maintain.

Preparation for Using NetBoot

If client computers use system software supplied by a NetBoot server, you can ensure that each computer has the same version of software and access to the same applications. Regardless of what users change during a session, the computers return to the same system configuration after restart. Network computers are easy to maintain because the user applications need to be installed only on a disk image stored on the server.

You must use the NetBoot Desktop Admin utility to change the Multiple Users control panel options so that NetBoot client computers retrieve account information from Macintosh Manager when they start up.

The steps below give a general description of how to prepare your managed network and clients for use with NetBoot. See the system image administration guide for more detailed information.

- Set up the client computers to start up from the Mac OS disk image on the server.
- Use Macintosh Manager to control user environment, preferences, and access to local and network resources.
- Install the Macintosh Manager server software on the server containing the Mac OS image that NetBoot client computers will use to start up. Use the same server to store users' documents and applications.
- Set up workgroup administrator accounts for certain users, such as teachers or technical staff, then show them how to use Macintosh Manager to manage user accounts and workgroups.

Setting Up Mac OS 9 Managed Clients

The following steps provide an overview of the initial setup process for managing clients in Macintosh Manager. Detailed information and tasks related to each part of the process are contained in other sections of this chapter as indicated by page references.

Step 1: Make sure Macintosh Manager services are available

Before you can take advantage of Macintosh Manager features, you must make sure the service has been started from the server.

To start Macintosh Manager service:

1. Open Server Admin and enter an administrator name and password.
2. Select a server in the Computers & Services list.
3. Click Settings, click Advanced, and select the Enable Macintosh Manager checkbox.

Step 2: Log in to Macintosh Manager Admin as an administrator

For instructions, see "Logging In to Macintosh Manager as an Administrator" on page 187.

Step 3: Import user accounts

You can import user accounts from Workgroup Manager or from a text file, and you can use a template to apply settings. Macintosh Manager provides a Guest account. You can also use the All Other Users account to provide access to unimported users.

For more information about working with user accounts, see "Importing User Accounts" on page 188.

Step 4: Designate a Macintosh Manager administrator

For instructions, see "Designating Administrators" on page 193.

Step 5: Designate workgroup administrators

For instructions, see "Designating Administrators" on page 193.

Step 6: Create workgroups for users

Workgroups let you group users together and apply the same settings to all the users. You can set up workgroups according to any criteria, such as purpose (video production) or location (a fourth-grade classroom), and provide users with convenient access to necessary resources. You can also use a template to apply workgroup settings.

For more information about creating workgroups, see "Setting Up Workgroups" on page 197.

Step 7: Create computer lists

Computer lists let you group computers and apply the same settings to all the computers. You can use a template to apply settings to a computer list. The All Other Computers account lets you provide managed network access to computers that aren't in a computer list.

For more information about using computer lists, see "Setting Up Computer Lists" on page 213.

Step 8: Select global settings and set up managed preferences folders

In addition to various settings for users, workgroups, and computers, Macintosh Manager provides other security and CD-ROM settings in the Global pane. You can also manage user preferences by placing preference files in Forced, Initial, or Preserved preferences folders.

For information about using global settings, see "Using Global Security Settings" on page 224 and "Using Global CD-ROM Settings" on page 226.

For information about using managed preference folders, see "Managing Preferences" on page 227.

Logging In to Macintosh Manager as an Administrator

The first time you open the Macintosh Manager administrative software and log in, you can use your Mac OS X Server administrator account. Later on, you can still log in to the Macintosh Manager administrator software using that account or other Macintosh Manager administrator accounts that you set up.

Note: You must log in from a remote computer. You cannot use Macintosh Manager administrator software on the same computer that is the designated Macintosh Manager Server.

To log in to Macintosh Manager:

1. Click the Macintosh Manager icon in the Dock to open Macintosh Manager. To open Macintosh Manager from Workgroup Manager, click the Macintosh Manager icon and choose Open Macintosh Manager.
2. Enter your administrator account user name and password.

After you log in, you can add user accounts, create workgroups, create computer lists, designate administrators, and access and change Macintosh Management service settings.

Working With Macintosh Manager Preferences

Macintosh Manager preference settings let you choose a sorting method for users and workgroups and choose a format for exported reports. Only Macintosh Manager administrators can change these settings.

To change Macintosh Manager preferences:

1 Log in to Macintosh Manager.

2 Choose Preferences from the Macintosh Manager menu (in Mac OS X) or choose Preferences from the File menu (in Mac OS 9).

3 Select settings for sorting users (by either name or type).

4 Select settings for sorting workgroups (by either name or environment).

5 Select a format for reports exported to a text file (using either tabs or commas to separate information fields).

6 If you want to use templates for users, groups, or computers, select "Show template" to include the "template" item in the list of accounts.

Importing User Accounts

This section explains various ways to import users and apply user settings. All user accounts must be created before you can import or modify them using Macintosh Manager. You cannot create user accounts in Macintosh Manager. If you haven't already set up users, see Chapter 4, "Setting Up User Accounts," for information and instructions.

Macintosh Manager user accounts are for anyone who uses a computer in a managed environment. Most users don't require access to the Macintosh Manager administrator application. If you want to give certain users (for example, managers, teachers, and so forth) administrative privileges, read "Designating Administrators" on page 193 for details.

You select user settings and the user type in the Users pane of Macintosh Manager. You can select options manually or use a template to apply settings as users are imported.

Applying User Settings With a Template

You can create a template and use it to apply identical settings to multiple users at once during import. This makes it easy to start managing large numbers of users quickly.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To set up or change a user template:

1 In the Users pane of Macintosh Manager, select Template in the Imported Users list.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

2 In the Basic and Advanced panes, set options you want to use for the template, then click Save.

Importing All Users

If you have a small number of users in your Mac OS X Server database, you may want to import them to Macintosh Manager all at once. You can import up to 10,000 users with the Import All feature.

To import all users:

1 In Macintosh Manager, click Users.

2 Click Import All.

An individual Macintosh Manager user account is created for each imported user. Depending on the number of users imported, this process may take some time. You can also import users individually or in groups.

If you have more than 1,000 users to import, you may want to consider importing users from a text file.

Importing One or More Users

If necessary, you can import individual users or small groups of users. You must be using the Macintosh Manager administrator software in Mac OS X in order to import one user at a time. You cannot import one user at a time using Macintosh Manager on a Mac OS 9 computer.

To add one or more users to Macintosh Manager:

1 In Macintosh Manager, click Users.

2 Click Import.

3 If Workgroup Manager is not already open, a message about adding users appears. Click Open to open Workgroup Manager.

4 In Workgroup Manager, click Users & Groups, then select Show Users & Groups List.

5 In the Users & Groups List, select the user or users you want to import and drag them to the Imported Users list in Macintosh Manager. You may need to rearrange the windows so that you can see both lists.

If you can't find a user in the Users & Groups List, that user may not be in your Mac OS X Server directory.

If you have fewer than 10,000 users to import, you can also use the Import All feature.

Collecting User Information in a Text File

You can create a plain text file that contains user information and then use this file when you import users into Macintosh Manager. Your file must contain at least one of the following pieces of information about each user: user ID, user name, or short name. You don't need to list password information.

To collect user information in a text file:

1 Make sure each user in the file already exists in directory services. Information for missing users is ignored.

2 Make sure each line of user information is separated by a hard return.

If you have multiple items of user information on each line, make sure the items are separated by either commas or tabs.

3 Make sure the file is saved as plain text and has ".txt" at the end of the file name.

To reduce the likelihood of error, avoid mixing types of user information in the text file. For example, you could use only the user ID for each user.

Importing a List of Users From a Text File

Using a text file to import user information is a convenient way to start managing large numbers of users.

To import users from a text file:

1 In Macintosh Manager, click Users.

2 Choose Import User List from the File menu, then select the file you want to import.

3 In the Available Fields list, select the list item that matches the first item of user information in your text file, then click Add to add the item to the Import list.

For example, if the first item in your text file is the user ID, the first item you add to the Import list should be user ID. Do the same for other information you want to import.

4 Choose either tab or comma for the field delimiter, depending on how you separated pieces of user information in your text file.

5 Click Open Sample Import to preview imported information, or click OK to start the import.

If a user cannot be found, you will see a warning message. Users in the text file must be present in the directory services database before you can import them into Macintosh Manager.

Finding Specific Imported Users

You can use the Select Users By feature to search for Macintosh Manager users according to chosen criteria.

To search for users:

1 Open Macintosh Manager, then click Users.

2 If Template appears in the list of users, make sure it isn't selected.

3 Choose Select Users By from the Edit menu.

4 Select the kinds of search information you want to use.

If you select Comment, you can find users that have certain words in their comment fields.

Providing Quick Access to Unimported Users

If you want to allow user access to a managed network without having to set up user accounts, you can use the All Other Users feature, or you can set up a guest user account.

If portable computers require access to your network, you may also want to use the All Other Computers account.

Using Guest Accounts

In Macintosh Manager, you can create three types of "guest" accounts, all of which can be managed.

- **All Other Users**

  Using All Other Users is a quick way to provide access to large numbers of users and manage them without having to import them into Macintosh Manager. Users with existing Mac OS X user accounts can log in and access their own home directories, preferences, and documents. They have the privileges and environment you set up for the All Other Users Account. You can also set login settings for All Other Users and allow them to exceed printer quotas.

  For information about how to set up the All Other Users account, see "Providing Access to Unimported Mac OS X Server Users" on page 192.

- **Guest**

  When a user logs in as Guest, no password is required. Anyone can use the Guest account when it is available, whether he or she has a Macintosh Manager user account, a Mac OS X Server user account, or no account at all.

  All users logged in as Guest have the same privileges and preferences. Any settings you choose for the Guest account apply to all users who log in as Guest. You can set login settings and user storage quotas for guest users. You can also allow them to exceed printer quotas.

  For more information about using the guest user account, see "Setting Up a Guest User Account" on page 192.

- **All Other Computers**

  Any computer that is "unknown" or not in a Macintosh Manager computer list uses settings selected for the All Other Computers account. Allowing unknown, or "guest," computers is useful if you want to manage users who want to connect to your network using their own portable computers.

  For more information about how to set up the All Other Computers account, see "Setting Up the All Other Computers Account" on page 214.

Providing Access to Unimported Mac OS X Server Users

After you enable the All Other Users feature, Macintosh Manager creates the All Other Users account and makes it available in the Imported Users list. You can treat the All Other Users account like any other user account with its own workgroup and settings, with a few exceptions:

- Computer checkout is not allowed.
- Working offline at a client computer is not allowed.
- A disk quota is not enforced.

Using the All Other Users account is the quickest and most convenient way to grant authenticated access and set up customized environments for users without having to import them into Macintosh Manager. For example, in a school with a central user database, you can set up Macintosh Manager service in a computer lab using only the All Other Users account. Any user on campus who has a Mac OS X Server account can walk into the lab, log in, and access his or her home directory in a managed environment.

To set up the All Other Users account:

1. In Macintosh Manager, click Global, and then click Security.
2. Select Allow All Other Users and click Save.
3. Click Users and select All Other Users in the Imported Users list.
4. Select settings in the Basic and Advanced panes, then click Save.
5. Click Workgroups, add All Other Users to a workgroup, and give the workgroup a name.
6. Select settings for that workgroup, then click Save.
7. Click Computers and make computers available to the workgroup you just created.

With the All Other Users account, settings for computer checkout, working offline, and disk quotas are not allowed.

Setting Up a Guest User Account

Because the Guest account doesn't require individual user names and passwords for each user, it is a good choice for setting up a public computer or kiosk where users don't need to access their home directories.

After you enable the Guest account, Macintosh Manager creates the account and makes it available in the Imported Users list. Computer checkout and working offline at a client computer are not allowed.

As with any other user account, you can add the Guest account to a workgroup and apply Macintosh Manager settings, with a few exceptions:

- Computer checkout is not allowed.
- Working offline at a client computer is not allowed.

To set up the Guest account:

1 Open Macintosh Manager, click Global, and then click Security.

2 Select "Allow Guest access."

3 Click Users, and select Guest in the Imported Users list. In the Basic and Advanced panes, select the settings you want to use.

4 Click Workgroups. Create a workgroup for the Guest account, or select an existing workgroup and add Guest to the Workgroup Members list in the Members pane.

5 Provide access to computers by making one or more lists of computers available to these workgroups.

6 Click Save.

Designating Administrators

After you import user accounts, you'll need to give some users administrative privileges. For Macintosh Manager, the privilege hierarchy is similar to that of Workgroup Manager, but Macintosh Manager uses only two types of administrative accounts. Macintosh Manager workgroup administrators are similar to Workgroup Manager's directory domain administrators, but their privileges apply only to workgroups created in Macintosh Manager.

About Macintosh Manager Administrators

A Macintosh Manager administrator can import, edit, and delete user accounts and create workgroup administrators and additional Macintosh Manager administrators. A Macintosh Manager administrator can change any of the Macintosh Manager settings and, if allowed, can use his or her administrator password to log in as any user except another Macintosh Manager administrator.

A Macintosh Manager administrator's administrative privileges don't apply in Mac OS X Workgroup Manager tools. For example, a Macintosh Manager administrator cannot create user accounts in Workgroup Manager (unless he or she also has a Mac OS X Server administrator account).

Allowing Mac OS X Server Administrators to Use Macintosh Manager Accounts

Because Macintosh Manager is disconnected from data (other than the user ID) used by Workgroup Manager, Mac OS X Server administrator accounts are imported to Macintosh Manager as regular users. They may not be able to access their home directories when they log in to client computers, and they will not automatically have administrative privileges in Macintosh Manager. They cannot access the Macintosh Manager share point or set up managed preferences.

You should create a separate Mac OS X Server user account for any server administrators you want to include in Macintosh Manager, and then import those accounts. If you want a user to have administrator privileges in Macintosh Manager, set the user type to Macintosh Manager Administrator in the Basic pane of the Users pane. If you want to give these users full administrative privileges in Macintosh Manager, follow the instructions for "Creating a Macintosh Manager Administrator" on page 194.

About Workgroup Administrators

Workgroup administrators can add or modify user accounts and workgroups according to privileges assigned to them. Regardless of privileges, they cannot change a user's type or change access settings, and they cannot create Finder workgroups.

Workgroup administrators also have access to shared folders, such as hand-in folders, which can be used to collect documents from users. In a school environment, for example, teachers who are workgroup administrators can distribute and collect assignments over the network. A teacher can also make available various network resources, applications, and CDs that promote teaching objectives for the class.

Creating a Macintosh Manager Administrator

You should create at least one Macintosh Manager administrator to prevent users from bypassing security and changing to a different Macintosh Manager server.

When you import users who have server administrator privileges, they're imported as regular users. They will not automatically have administrative privileges in Macintosh Manager, but you can assign those privileges.

To designate a Macintosh Manager administrator:

1 In Macintosh Manager, click Users.

2 Select one or more users in the Imported Users list.

3 Change the user type to Macintosh Manager Administrator, then click Save.

To allow all Macintosh Manager administrators to use their passwords to log in as any user except another Macintosh Manager administrator, select "Users may log in using a server administrator's password" in the Security pane of the Global pane.

Creating a Workgroup Administrator

You can set up workgroup administrator accounts for people (such as teachers or technical coordinators) who may need to add or modify certain user accounts or workgroups.

To designate a workgroup administrator:

1 In Macintosh Manager, click Users.

2 Select one or more users in the Imported Users list.

3 Change the user type to Workgroup Administrator and click Save.

Changing Your Macintosh Manager Administrator Password

Macintosh Manager administrators can change their passwords whenever necessary.

To change your administrator password:

1 Log in to Macintosh Manager.

2 Choose Change Password from the Configure menu.

3 In the text fields provided, type your current password, then type your new password. Then, type your new password again to verify it.

Working With User Settings

This section describes basic and advanced user settings and how to use them. Available settings in the Advanced pane vary depending upon the user type. All users have the same options available for basic settings regardless of user type.

Changing Basic User Settings

Name, short name, and ID information is imported with each user. This information cannot be changed in Macintosh Manager. For information about how to change this information, see Chapter 4, "Setting Up User Accounts."

You can change basic settings for more than one user at a time. When you have multiple users selected, the name, short name, and ID change to "Varies."

To change basic user settings:

1 In Macintosh Manager, click Users, and then click Basic.

2 Select one or more users in the Imported Users list.

3 Choose a type from the User Type pop-up menu.

4 Select login settings.

"User can log in" is already selected. Deselect it if you want to disable user login immediately.

If you want to prevent a user from logging in after a specific date (for example, after a school session ends), select "Disable log-in as of __" and type a date.

5 Add comments (up to 63 characters long) in the Comments field.

This is a good place to put user-specific information (for example, a student's grade level or an employee's office location) or keywords that will help you find users.

6 Click Save.

Allowing Multiple Logins for Users

Ordinarily, users must log out on one computer before they can log in on another. However, you may want to allow certain users, such as technical support staff or administrators, to log in on several computers simultaneously (to do maintenance tasks, for example).

To allow simultaneous logins:

1 In Macintosh Manager, click Users, and then click Advanced.

2 Select a user in the Imported Users list.

3 Deselect "User can only log in at one computer at a time."

4 Click Save.

Granting a User System Access

Users who have system access can access all items on a client computer, including the Finder and the System Folder. Grant system access to specific users, such as workgroup administrators or technical support staff, only if necessary. Macintosh Manager administrators always have system access.

To allow system access for a user:

1 In Macintosh Manager, click Users, and then click Advanced.

2 Select a regular user or workgroup administrator in the Imported Users list.

3 Select "User has system access."

4 Click Save.

Changing Advanced Settings

Depending upon the user type, some advanced settings may or may not be available. Also, workgroup administrators cannot change access settings, email settings, or user type.

To change advanced settings for a user:

1 In Macintosh Manager, click Users, and then click Advanced.

2 Select the user or users you want to modify in the Imported Users list.

You can select multiple users, but they should be of the same type. If you select different types of users, you will be able to modify only the advanced settings that those users have in common.

3 Select access settings and set quotas.

Initially, users of all types can log in to only one computer at a time. No other settings are selected.

4 If the user is a workgroup administrator, select the privileges you want the user to have under "Allow this Workgroup Administrator to." Initially, no privileges are selected.

5 Click Save.

Limiting a User's Disk Storage Space

A disk space quota limits the amount of storage space available in a user's home directory. Once a user exceeds the storage limit, he or she cannot save any more files there. Users see a warning message if they run out of storage space.

To set a user storage quota:

1. In Macintosh Manager, click Users, and then click Advanced.
2. Select a user in the Imported Users list.
3. Select "Set user storage quota to __ K" and type the maximum amount of storage space to allow in kilobytes (1024 kilobytes = 1 megabyte).

   When you set a storage quota, keep in mind the amount of space available and the number of users who will share it.
4. To allow a user to save files even if he or she exceeds the set quota, select "Only warn user if they exceed this limit."
5. Click Save.

Updating User Information From Mac OS X Server

If you change user information in Workgroup Manager or delete user accounts, you need to synchronize Macintosh Manager with the Mac OS X Server database to make sure user data is the same in both places.

To update Macintosh Manager user data:

1. In Macintosh Manager, click Users.
2. Choose Verify Users & Workgroups from the File menu.

If the user account exists in the server database, Macintosh Manager updates the user's information to match information in the server database. For very large numbers of users, this process can take some time.

Note: If the user account can't be found, the user is deleted from Macintosh Manager.

Setting Up Workgroups

In the Members pane of the Workgroups pane, you can create new workgroups, change an existing workgroup's name or type, and add or remove workgroup members.

Important: If a user is not a workgroup member, he or she cannot log in to the Macintosh Manager network. Group accounts are not imported from Workgroup Manager; you must create them. Every managed user must belong to at least one workgroup. Users can belong to more than one workgroup, but users can select only one workgroup when they log in.

This section describes the different workgroup environments and tells you how to apply workgroup settings manually, by duplicating a workgroup, and by using a template.

Types of Workgroup Environments

Workgroups can have one of three types of desktop environments. All three types have some optional settings in common. Important differences are described below.

- **Finder workgroups have the standard Mac OS desktop.**
  The System Folder and Applications folder are not automatically protected, but you can choose to protect them. Members of Finder workgroups have no restrictions on the File menu, Apple menu, or Special menu. They also have no restrictions on removable media or CDs.
- **Restricted Finder workgroups have the standard Mac OS desktop, but with restrictions.**
  The System Folder and the Applications folder are protected. This means users can view the contents, but cannot modify them or add new items. Users can access File menu and Special menu items, but you can choose available items for the Apple menu. You can also control the user's ability to take screen shots, and you can choose privileges for CDs, removable media, and shared folders.
- **Panels workgroups have a simplified interface with large icons that make using a computer easy for novice users, particularly children.**
  Panels workgroup options are the same as Restricted Finder options, with a few additions. You can control access to the File menu and the Special menu in addition to the Apple menu, and you can select whether or not to show a mounted volume as a panel. Members of a Panels workgroup cannot view items on the local hard disk.

Creating a Workgroup

Workgroup members can be of any user type, and workgroups can have up to 1500 members. Workgroup administrators, if allowed, can create Restricted Finder and Panels workgroups, but they cannot create Finder workgroups.

To create a workgroup:

1. In Macintosh Manager, click Workgroups.
2. Click New and type a name for the workgroup.
3. Choose an environment type from the Environment pop-up menu.
4. Select one or more users in the Available Users list and click Add.

   To remove workgroup members, select the users you want to remove in the Workgroup Members list, then click Remove.
5. Choose settings for this workgroup in the other panes, then click Save.

You can duplicate workgroups or use a template to apply settings to new workgroups.

Using a Template to Apply Workgroup Settings

You can use a template to quickly create several workgroups that have the same settings. Once you modify the template, each new workgroup you create will have the template settings. You can make additional changes to the workgroup after it is created.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To set up or change a template:

1 In Macintosh Manager, click Workgroups.

2 Select Template in the Workgroups list.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

3 In each of the Workgroup panes, set the options you want to use in the template, then click Save.

Creating Workgroups From an Existing Workgroup

Duplicating an existing workgroup is a quick way to create another Macintosh Manager workgroup that already has settings or members you want.

To duplicate a workgroup:

1 In Macintosh Manager, click Workgroups. Then select a workgroup in the Workgroups list.

2 Click Duplicate and type a new name for the workgroup.

3 Add or remove members and change settings if you wish, then click Save.

You can also use a template to apply preselected settings to a new workgroup.

Modifying an Existing Workgroup

After a workgroup is created, you can change its name or environment type and add or remove members. A workgroup administrator can change settings for a workgroup only if he or she is also a member of that workgroup.

To change Members settings:

1 In Macintosh Manager, click Workgroups, and then click Members.

2 Change the workgroup name in the text field.

3 Choose a new environment from the pop-up menu.

Workgroup administrators cannot select Finder as a workgroup environment.

4 To add new members, select one or more users in the Available Users list and click Add. To remove members, select members in the Workgroup Members list, and click Remove.

5 Click Save.

Using Items Settings

Items settings let you make files and applications on client computers available to workgroup members.

Setting Up Shortcuts to Items for Finder Workgroups

You can use settings in the Items pane to create a list of applications, folders, and files that workgroups can access. If you choose to allow access to local items, the items appear in the Shortcut Items list. Macintosh Manager creates an alias for each item in the list.

Aliases for shortcut items appear on the user's desktop. When users log in, their computers look for the original file in the "Find chosen items" location and create an alias for the file.

Important: Unless you plan to look for original items only on local volumes, be sure personal file sharing is turned off and other Apple Filing Protocol (AFP) services are not running before you proceed. Alternatively, use a computer that has Macintosh Manager, but not file service, installed.

To make items on the local volume available to a workgroup:

1 In Macintosh Manager, click Workgroups, and then click Items.

2 Select "Members can open any items on local volumes" if you want to allow access to items stored on the computer where users are logged in.

If you select this option, access is not restricted, but you can use Shortcut Items to provide quick access to a particular set of applications, folders, and/or files.

3 Choose a volume from the Volume pop-up menu.

4 Select items in the Volume list that you want to add to the Shortcut Items list and click Add.

To remove items from the Shortcut Items list, select them and click Remove. Use Find to search for additional items, such as files or folders.

5 Choose a location from the "Find chosen items" pop-up menu.

A user's computer looks for the original file in this location, and then downloads the alias.

6 Click Save.

Making Items Available to Panels or Restricted Finder Workgroups

You can use settings in the Items pane to create a list of applications, folders, and files that workgroups can access. If you choose to allow access to only specific items, the items appear in the Approved Items list. Macintosh Manager creates an alias for each item in the list.

Aliases for approved items appear either on a panel for Panels workgroups or in a folder on the desktop for Restricted Finder workgroups. When users log in, their computers look for the original file in the "Find chosen items" location and create an alias for the file.

Important: Unless you plan to look for original items only on local volumes, be sure personal file sharing is turned off and other AFP services are not running before you proceed. Alternatively, use a computer that has Macintosh Manager, but not file service, installed.

To provide access to applications and other items:

1 In Macintosh Manager, click Workgroups, and then click Items.

2 Select an application access setting.

Select "Members can open any items on local volumes" if you want to allow access to items stored on the computer where users are logged in. If you select this option, access is not restricted, but you can use Shortcut Items to provide quick access to a particular set of applications, folders, and/or files.

Select "Allow members to open only the following items" if you want to allow access to only certain approved applications, folders, or files.

3 Choose a volume from the Volume pop-up menu.

4 Select items in the Volume list that you want to add to the Approved Items or Shortcut Items list, and click Add. You can also drag items directly into the list.

To remove items from the list, select them and click Remove. Use Find to search for additional items, such as files or folders.

5 Choose a location from the "Find chosen items" pop-up menu.

When a user attempts to open a Shortcut Items or Approved Items alias, the computer looks for the original file in the "Find chosen items" location.

The computer can search local volumes and mounted server volumes. If the original item is on a server volume that is not mounted, the computer won't be able to find it.

For a NetBoot client computer, a local volume is the hard disk in the computer or any external hard disk connected directly to the computer. The startup volume for a NetBoot client computer is a remote volume, but it is treated as a local volume.

6 Click Save.

Making Items Available to Individual Users

In some cases, you may want to make specific documents or applications available to individual users. For example, a user working on a special video project may require a video-editing application that other workgroup members don't need.

To make items available to a specific user:

- Place the items in the user's home directory.

Using Privileges Settings

Settings in the Privileges pane allow you to enable certain security measures, control access privileges for workgroup folders, and set options to allow users to take screen shots, play audio CDs, and open items on removable media. Available privilege settings vary depending upon the type of workgroup selected in the Workgroups list. If you have more than one type of workgroup selected when you make changes, you will be able to change only those settings that the workgroups have in common.

Protecting the System Folder and Applications Folder

For Panels and Restricted Finder workgroups, these folders are always locked. Users can view the contents, but cannot make changes. Finder workgroups don't automatically have these folders protected, but you can set these restrictions.

To protect these folders:

1. In Macintosh Manager, click Workgroups, and then click Privileges.
2. Select a Finder workgroup in the Workgroups list.
3. Click the checkboxes next to System Folder and Applications folder to protect them.
4. Click Save.

Protecting the User's Desktop

You can prevent users from storing files or folders on the desktop and changing the desktop pattern, icon arrangement, or other desktop settings.

To protect the desktop:

1. In Macintosh Manager, click Workgroups, and then click Privileges.
2. Select a workgroup in the Workgroups list.
3. Click the checkbox to select "Lock the user's desktop on the startup volume."
4. Click Save.

Preventing Applications From Altering Files

Enforcing file-level security prevents applications from writing to protected folders and files, but it may cause some older applications to report disk errors or have problems opening. If you don't enforce file-level security, applications can write information (for example, temporary data or preferences) wherever necessary.

File-level security is available only for Mac OS 9 clients and applies only to applications. It doesn't affect user access to folders and files.

To enable file-level security:

1 In Macintosh Manager, click Workgroups, and then click Privileges.

2 Select a workgroup in the Workgroups list.

3 Select "Enable file level security for Mac OS 9 workstations," then click Save.

Preventing Access to FireWire Disks

You can enable file-level security to prevent users in a Panels workgroup from accessing FireWire hard disks that are mounted at startup. This applies only to Mac OS 9 clients and doesn't affect Finder or Restricted Finder workgroups.

To enable file-level security to prevent access to FireWire disks:

1 In Macintosh Manager, click Workgroups, and then click Privileges.

2 Select a Panels workgroup in the Workgroups list.

3 Select "Enable file level security for Mac OS 9 workstations," then click Save.

Allowing Users to Play Audio CDs

Users in a Finder workgroup can always play audio CDs. Panels or Restricted Finder workgroups don't automatically have that privilege, but you can give it to them.

To allow users to play audio CDs:

1 In Macintosh Manager, click Workgroups, and then click Privileges.

2 Select a Panels or Restricted Finder workgroup in the Workgroups list.

3 Select "Play audio CDs," then click Save.

Some CDs contain more than just audio tracks. If the first track on a CD is an audio track, then it is an audio CD.

Allowing Users to Take Screen Shots

Special key combinations let users take a picture of the computer screen (called a "screen shot") and save the picture as a file stored in the user's Documents folder. Users in Finder workgroups are always allowed to take screen shots. Panels or Restricted Finder workgroups don't automatically have this privilege, but you can give it to them.

To allow users to take screen shots:

1 In Macintosh Manager, click Workgroups, and then click Privileges.

2 Select a Panels or Restricted Finder workgroup in the Workgroups list.

3 Select "Take Screen Shots," then click Save.

If disk space is a concern, you may not want to enable this feature.

For information about how to take screen shots, see Mac Help.

Allowing Users to Open Applications From a Disk

If you use a list of "approved items" (applications or scripts) that users can access, users in a Panels or Restricted Finder workgroup cannot open applications on removable media (for example, floppy disks) unless you allow it.

Finder workgroups don't have this restriction.

To allow users to open applications on removable media:

1. In Macintosh Manager, click Workgroups, and then click Privileges.
2. Select a Panels or Restricted Finder workgroup in the Workgroups list.
3. Select "Open approved items on removable media," then click Save.

Removable media include floppy disks, Zip disks, and all other types of removable media except CDs or DVDs.

You can set up a list of approved items in the Items pane of the Workgroups pane.

Setting Access Privileges for Removable Media

For Panels and Restricted Finder workgroups, you can set access privileges for removable media. Removable media include floppy disks, Zip disks, and all other types of removable media except CDs.

To set privileges for removable media, other than CDs:

1. In Macintosh Manager, click Workgroups, and then click Privileges.
2. Select a Panels or Restricted Finder workgroup in the Workgroups list.
3. Choose an access privilege setting from the pop-up menu next to "Removable media (except CDs)," then click Save.

Setting Access Privileges for Menu Items

For certain Finder menus, you can decide which menu items users can see. For Panels workgroups, you can control items in the Apple menu, File menu, and Special menu. For Restricted Finder workgroups, you can only control items in the Apple menu and the Special menu. Finder workgroups don't have these restrictions.

To set privileges for menu items:

1. In Macintosh Manager, click Workgroups, and then click Privileges.
2. Select a Panels or Restricted Finder workgroup in the Workgroups list.
3. Select each menu item you want workgroup members to be able to use, then click Save.

Sharing Information in Macintosh Manager

Macintosh Manager provides a number of ways to share information among users or workgroups by using different types of shared folders. Most shared folders are created inside the group documents volume. Some folders are created automatically, but others must be created by the administrator.

Types of Shared Folders

- *Workgroup shared folder:* Only members of a single workgroup can use this folder. When you set up a group documents volume, a shared folder is automatically created the first time a user logs in to the workgroup.
- *Global shared folder:* Members of all workgroups whose workgroup folder is on the same volume can access this folder, allowing documents to be shared between workgroups. A global shared folder is automatically created when you select a group documents volume.
- *Workgroup hand-in folder:* A hand-in folder is automatically created the first time a user logs in to the workgroup (provided that the privileges have been set up). Hand-in folders are available only to Panels and Restricted Finder workgroups. The hand-in folder is stored on the group documents volume. At least one workgroup administrator or Macintosh Manager administrator must be a member of the workgroup to use this feature because only an administrator can see items in the hand-in folder.

  Workgroup members put items into the folder by choosing Hand In from the File menu (in the Panels environment) or by dragging the item to the hand-in folder (in the Restricted Finder environment).
- *Folder on the startup disk named ___:* A Macintosh Manager administrator can create a folder at the top level of the startup disk and then allow users to open items stored in that folder. This type of folder is useful for storing items that workgroup members need to access easily or frequently, such as clip art.

Folder Access Privileges

Macintosh Manager allows four levels of access privileges for workgroup folders:

Access setting	What it means
Read Only	Users can view and open items in the folder, but they cannot modify them, and they cannot "write to" the folder. For example, they cannot save a file in the folder.
Write Only	Users cannot view or open items in the folder, but they can write information to the folder. For example, they can copy a document to the folder.
Read & Write	Users have unrestricted access to the folder. They can view, open, modify, or write information to the folder.
No Privileges	Users cannot do anything at all with the folder.

Selecting Privileges for Workgroup Folders

After you create a group documents volume, you can set user access privileges (Read Only, Write Only, Read & Write, or No Privileges) for various workgroup folders.

To set access privileges for workgroup folders:

1. Make sure the group documents volume is already set up before you proceed.
2. In Macintosh Manager, click Workgroups, and then click Options.
3. Select a Panels or Restricted Finder workgroup.
4. Choose an access privilege setting from the pop-up menu next to each type of folder that is available for the workgroup.
5. Click Save.

Setting Up a Shared Workgroup Folder

A shared workgroup folder is a convenient location where workgroup members can store and share any kind of information, depending on how file and folder access privileges are configured. For example, if you set up Read & Write privileges for a shared group documents volume, several users can share HTML files or images for a collaborative project.

To set up a group documents folder:

1. Open Macintosh Manager.

   Before you proceed, make sure the group documents settings in the Options pane are correct. If they're not, choose the correct group documents location and login settings, and then click Save.

2. Click Workgroups, then click Privileges.
3. Select one or more workgroups in the Workgroups list.
4. In the Privileges section, set "Workgroup shared folder" to Read & Write, then click Save.

   If you want to prevent users from changing the documents in the workgroup shared folder, you can lock each document. To learn how to lock a document, see Mac Help.

Setting Up a Hand-In Folder

A hand-in folder works like a drop box. Users can save items in the folder, but they can't see any items in the folder. Hand-in folders are very useful for collecting and protecting sensitive documents. For example, in a classroom, students can turn in homework by copying their files into the folder. Employees in a workplace can place status reports or personal reviews in a hand-in folder that only their managers can access.

Hand-in folders are available only for Panels or Restricted Finder workgroups.

To create a hand-in folder:

1 Open Macintosh Manager, click Workgroups, and then click Options.

Before you proceed, make sure the group documents settings in the Options pane are correct. If they're not, choose the correct group documents location and login settings, then click Save.

2 Click Workgroups, then click Privileges.

3 Select one or more Panels or Restricted Finder workgroups in the Workgroups list.

4 In the Privileges section, set "Workgroup hand-in folder" to Write Only, then click Save.

The hand-in folder appears as an item in the File menu for Panels workgroups. For Restricted Finder workgroups and workgroup administrators, it appears as a folder on the desktop.

Using Volumes Settings

You can use the Volumes settings for Workgroups to select which volumes are mounted when users log in and control login options for each volume. A volume is a shared folder on a file server.

Connecting to AFP Servers

Mac OS X Server supports TCP/IP network connections to Apple Filing Protocol (AFP) servers such as the Macintosh Manager server. You cannot use AppleTalk connections to AFP servers.

Providing Access to Server Volumes

If workgroup members need to use files and applications that are not stored on the Macintosh Manager server, you can mount volumes automatically when users log in.

Even if you don't set up a server volume to mount automatically, users can still connect to it if they have access to the network and have an account on (or guest access to) that server.

To connect to volumes automatically:

1 In Macintosh Manager, click Workgroups, and then click Volumes.

2 Select one or more workgroups.

3 Select a volume in the Volumes list, then click Add.

If you don't see the volume you want, click Find and locate the volume.

When the volume is mounted, it requests a login name and password.

4 Select a volume in the "Mount at Log-in" list and choose login settings (explained in the steps that follow).

5 If the volume doesn't use the same user names and passwords used by Macintosh Manager, select "Prompt user for log-in." Users must enter a valid user name and password.

6 If you want to grant easy access to a volume for all users, select "Log in automatically as this AFP user" and type in a valid user name and password.

This isn't as secure as requiring users to log in with their own information, because you can't control access individually or track who has logged in to the server.

You can select "Always try automatic log-in with user's name and password first" in addition to the other login settings.

If this attempt at login fails, the login method you selected under "When mounting" is used.

7 Select "Use AFP privileges" to use Apple Filing Protocol read and write permission settings to determine access privileges for a particular volume. Ordinarily, Macintosh Manager allows read-only access to volumes.

This setting doesn't apply to Finder workgroups.

8 If you select "Require an administrator password to unmount," users can't disconnect the volume unless they have the correct password.

This setting doesn't apply to Finder workgroups.

9 For Panels workgroups only, select "Show volume on a panel" if you want the user to see the volume icon.

If you don't select this option, the volume can only be seen in the Applications panel.

10 Click Save.

Using Printers Settings

Printers settings let you control access to workgroup printers and limit the number of pages printed. Some settings are available only if you select "Allow members to use only the following Desktop Printers."

Making Printers Available to Workgroups

Before you can make a printer available to a workgroup, the printer must appear in the Available Printers list. You can add printers using Create New in the Printers pane of the Workgroups pane, or you can add them in the Printer Setup Utility application (in Mac OS X) on the Macintosh Manager server.

Note: The Mac OS X version of the Macintosh Manager administrator application only creates LaserWriter desktop printers. In order to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients. To add printers in Mac OS 9, use the Chooser in the Apple menu.

To allow access to printers:

1 In Macintosh Manager, click Workgroups, and then click Printers.

2 Make sure "Allow members to use only the following Desktop Printers" is selected.

3 Select one or more printers in the Available Printers list and click Add.

4 When you have finished adding printers, click Save.

You cannot grant access to both the system access printer and desktop printers. If you want a workgroup to use the system access printer, log in to the System Access workgroup as an administrator and use the Chooser to select a printer. Then follow the steps above.

Setting a Default Printer

When a user prints a document, applications prefer to send the document to the default printer. If multiple printers are available, the user has the opportunity to select a different printer.

After printers have been added to the Available Printers list, you can determine how applications will know which printer to use first.

To select a default printer:

1 In Macintosh Manager, click Workgroups, and then click Printers.

2 Make sure "Allow members to use only the following Desktop Printers" is selected.

3 Select a printer in the Selected Printers list and click Set Default Printer.

If multiple printers are available and you select "Remember last used printer," applications prefer to send print jobs to the last printer used, even if it isn't the default printer. The user still has the opportunity to select a different printer.

Restricting Access to Printers

You can restrict access to a printer by removing it from the Selected Printers list or by requiring a password to use it.

To restrict access to a printer:

1 In Macintosh Manager, click Workgroups, and then click Printers.

2 Make sure "Allow members to use only the following Desktop Printers" is selected.

3 Select a printer in the Selected Printers list. If you want to remove the printer from the list, click Remove.

4 Select "Require an administrator password to print to this printer" to protect only the selected printer. To password-protect all printers in the list, select "Require an administrator password to print to any printer."

Setting Print Quotas

A print quota limits the number of pages a user is allowed to print over a period of time. The number of pages allowed refers to the document's page count, not to the number of pieces of paper. For example, if you print a 16-page document using a layout that shows four document pages on each printed page, you'll use four sheets of paper; however, 16 pages are subtracted from your print quota. Pages are counted against the maximum allowance even if the printing job is not completed (for example, if there is a paper jam).

Using a print quota helps encourage users to use printing resources wisely and helps decrease waste. You can set an individual quota for each printer in the Selected Printers list.

To set a print quota for a user:

1. In Macintosh Manager, click Workgroups, and then click Printers.
2. Make sure "Allow members to use only the following Desktop Printers" is selected.
3. Select a printer in the Selected Printers list.
4. Select "Limit users to no more than __ pages every __ days" and enter the maximum number of pages to allow in a number of days.
5. Click Save.

Allowing Users to Exceed Print Quotas

When you set a print quota, the limitation applies to every user in the selected workgroup. However, you can allow certain users to ignore all print quotas.

To allow a user to exceed all print quotas:

1. In Macintosh Manager, click Users, and then click Advanced.
2. Select a user in the Imported Users list, then select "Allow user to exceed print quotas."
3. Click Save.

Setting Up a System Access Printer

If the printer you want to use doesn't support desktop printing software, you can make the printer available as a system access printer. The system access printer becomes the default printer for the selected workgroup.

Users who can see the Chooser can select any printer visible to them. When the user logs out of a client computer, the printer originally chosen by the administrator as the system access printer becomes the default printer again.

Note: You cannot use both regular desktop printers and a system access printer.

To set up a system access printer:

1. Create one or more computer lists containing client computers on which you plan to use system access printers.
2. For each workgroup you want to use a system access printer, make sure that workgroup has access to the computers in the list or lists you created.
3. Log in to a client computer using the System Access workgroup.

   You see the System Access workgroup only if you're a Macintosh Manager administrator or if "User has System Access" is enabled for your account.
4. Select Chooser from the Apple menu.
5. Select and set up a printer, then choose Quit from the File menu and log out.
6. Repeat steps 3 through 5 for each client computer on which users need access to a system access printer.
7. From the server or an administrator computer, open Macintosh Manager.
8. Click Workgroups, then click Printers.
9. Select a workgroup that has access to the computers you set up in the previous steps.
10. Select "Members use printer selected in System Access."
11. Click Save.

If you specify that a workgroup should use the system access printer, but don't select a printer from a client computer, users who log in to that computer will not be able to print unless they have access to the Chooser.

Using Options Settings

Options settings are used to set up a group documents folder, create a login message for workgroups, set startup and login events, and allow users in Panels or Restricted Finder workgroups to eject CDs.

Choosing a Location for Storing Group Documents

You can use specify a place (a volume) to store folders and files you want to make available to everyone in a workgroup. Once you have chosen a location and login settings for the group documents volume, you can set up shared folder access in the Privileges pane.

To set up a group documents volume:

1. In Macintosh Manager, click Workgroups, and then click Options.
2. Choose a location for storing group documents from the "Stored on volume" pop-up menu.

3 If the volume doesn't use the same user names and passwords used by Macintosh Manager, select "Prompt user for log-in."

Users must enter a valid user name and password.

4 If you want to grant easy access to the group documents volume for all users, select "Log in automatically as this AFP user" and type a valid user name and password.

This isn't as secure as requiring users to log in with their own information, because you can't control access individually or track who has logged in to the server.

5 If the group documents location is "Designated Macintosh Management Server," you can choose "Log-in Automatically using the default name and password."

The default name and password are internal to Macintosh Manager. You cannot track user login if you choose this setting.

You can select "Always try automatic log-in with user's name and password first" in addition to the other settings. If this attempt at login fails, the login method you selected under "When mounting" is used.

6 Click Save.

If the location you want doesn't appear in the menu, choose Other from the "Stored on volume" pop-up menu. You can select only volumes that are mounted on the server. If you still can't find the volume you want, click Find and mount the appropriate volume (available in Mac OS 9 only).

Making Items Open at Startup

You can give users a head start on their work by conveniently opening applications or folders for them when the computer starts up. On Mac OS 9 computers (using the MMLocalPrefs extension), follow the steps below to set up and enable startup items.

To open items at startup:

1 Before you enable the Startup Items option for Macintosh Manager clients, make sure you place the items you want to open at startup in the correct location.

On Mac OS 9 computers, place items in the user's personal Startup Items folder located on the server at /Library/Classic/Startup Items inside the user's home directory. Don't place items in the local Mac OS 9 System Folder.

2 In Macintosh Manager, click Workgroups, and then click Options.

3 Select one or more workgroups in the Workgroups list.

4 Select "Open items in the Startup Items folder" and click Save.

For computers that start up using NetBoot, you must follow special procedures to copy items to the Startup Items folder on the startup disk image. See the system image administration guide for details.

Checking for Email When Users Log In

If a user has a Post Office Protocol (POP) email account, you can have Macintosh Manager check the mail server for messages when the user logs in.

To check for email automatically:

1 Open Macintosh Manager.

Before you proceed, click Computers, and then click Control. Check the incoming email server information and make sure it is correct. The incoming email server must be a POP server in order to check email at login.

2 Click Workgroups, then click Options.

3 Select "Check for email when members log in," then click Save.

Creating Login Messages for Workgroups

You can display a message or announcement when a user logs in.

To create a workgroup login message:

1 In Macintosh Manager, click Workgroups, and then click Options.

2 Type a message in the Group Message box, then click Save.

Setting Up Computer Lists

You can use Macintosh Manager to manage computers by grouping several computers together and choosing settings for them. Once you create a list of computers you want to manage, you can select workgroups that are allowed to use them, and you can customize control settings, security settings, and login settings for each list. Checkout features are used to manage portable computers such as iBooks.

This section tells you how to set up computer lists individually, by duplication, or by using a template.

Creating Computer Lists

Computer lists are simply groups of computers, in the same way that workgroups are groups of users. These lists appear under "Machine Lists" on the left side of the Computers pane. You can limit access to computers by assigning specific workgroups to the computers you want them to use. Computer lists are also useful if you want certain computers to have different settings.

A computer cannot belong to more than one list.

To set up a computer list:

1 In Macintosh Manager, click Computers, and then click Lists.

2 Click Add and give the new list a name.

The name can contain up to 31 characters (including period, underscore, dash, or space). The name cannot contain a colon (:).

3 Click Find and choose or connect to a computer from the workstation selection window.

Repeat this step for each computer you want to appear in the list. To remove a computer from the list, select it and click Remove.

4 Make sure the login option is set to Enabled. Choose additional settings for the computer list in the other Computers panes, then click Save.

Note: If you use Macintosh Manager to manage a computer named using Japanese characters, the name in the list on the Computers/Lists pane in Macintosh Manager is garbled.

Setting Up the All Other Computers Account

Any settings selected for All Other Computers are applied to computers that connect to your managed network but don't appear in their own computer lists. These computers are also called guest computers.

To set up the All Other Computers account:

1 In Macintosh Manager, click Computers.

2 Select the All Other Computers account.

3 Choose the settings you want to use in each pane of the Computers pane, then click Save.

Duplicating a Computer List

You can easily create a computer list with the same settings as one you have already created. A duplicate list doesn't contain any computers because a computer cannot be in more than one list, but the settings are the same as the original.

To duplicate a computer list:

1 In Macintosh Manager, click Computers, and then click Lists.

2 Select an existing computer list and click Duplicate.

3 Type a new name for the list, then click Add to add computers to the list.

4 Click Save.

Creating a Computer List Template

You can use a template to apply the same initial settings to new computer lists. After you set up the template, each new computer list you add will have the template settings. You can change the computer list settings or the template settings at any time.

You cannot add computers to a template because computers cannot belong to more than one list.

Note: Once you set up a template, you cannot reset it to its original state. You can, however, change template settings any time you want.

To create a template for computer lists:

1 In Macintosh Manager, click Computers, and then select Template in the list of computer lists.

If you don't see the template, open Macintosh Manager Preferences and make sure "Show templates" is selected.

To open Macintosh Manager Preferences in Mac OS X, choose Preferences from the Macintosh Manager menu. In Mac OS 9, choose Preferences from the Edit menu.

2 In each Computers pane, set options you want to use for the template, then click Save.

Disabling Login for Computers

Occasionally, you may need to prevent user access on certain computers while you do maintenance tasks, such as installing and updating applications or running hard disk maintenance software. You can prevent access to computers by disabling login.

To prevent users from logging in on certain computers:

1 In Macintosh Manager, click Computers, and then click List.

2 Select a computer list, then set one of the login options explained in the steps that follow.

3 Select "Disabled--Ask User" to allow the user to choose to shut down the computer, go to the Finder (if the user has an administrator password), or pick a new Macintosh Manager server.

4 Select "Disabled--Go to Finder" to take the user to the Finder automatically.

5 Select "Disabled--Pick a different server" to allow the user to select another Macintosh Manager server from a list of local network servers.

6 Click Save.

To allow users to log in again, choose Enabled from the login pop-up menu and click Save.

Using Workgroup Settings for Computers

You use settings in the Workgroups pane of the Computers pane to control access to computers.

Controlling Access to Computers

You can make computers available to everyone, or you can limit access to certain computers. If you want to allow specific workgroups to use only certain computers, make sure you have already set up the workgroups first. Then create a list of computers you want to make available to them, and follow the steps below.

The same workgroup can be added to more than one computer list.

To make computers available to workgroups:

1 In Macintosh Manager, click Computers, and then click Workgroups.

2 If you want to make computers available to everyone, select "All workgroups can use these computers." To limit access to only certain workgroups, select "Allow only the following workgroups to use these computers."

3 Select workgroups in the Available Workgroups list and click Add to add them to the Allowed Workgroups list. To remove an allowed workgroup, select it and click Remove.

4 Click Save.

If you want to disable access to certain computers, use one of the "disabled" login settings in the Lists pane of the Computers pane.

Using Control Settings

Control settings are used to set email settings in addition to options that affect the clock, hard disk name, and automatic disconnect.

Disconnecting Computers Automatically to Minimize Network Traffic

While a computer is connected to a network, even if no user is logged in, it looks for updates to databases on the server at regular intervals. On very large networks, you may notice delays in client response. You can ease the burden on your network by scheduling an automatic disconnect for computers when they're not in use.

To enable automatic disconnect:

1 In Macintosh Manager, click Computer, and then click Control.

2 Select a computer list, then select "Disconnect from the server if no user logs in within __ minutes."

3 Type in how many minutes the computer should wait before disconnecting.

4 Click Save.

When the computer disconnects from the server, the computer still displays the login screen, but an X appears over the server icon in the menu bar. Automatic updates will not occur again until a user logs in.

To reconnect a client, select a user and click Login. Then, click Cancel in the password dialog.

Setting the Computer Clock Using the Server Clock

If your network doesn't have access to a Network Time Protocol server, you can synchronize the clocks on managed computers with the clock on the server.

To synchronize computer clocks:

1 In Macintosh Manager, click Computers, and then click Control.

2 Select a computer list, then select "Synchronize computer clocks with the server's clock."

3 Click Save.

Using a Specific Hard Disk Name

Specifying a certain name for a computer's hard disk can make it easier for some applications to locate information, such as preferences. Using a specific hard disk name is particularly useful if you use NetBoot. NetBoot clients have a startup volume named "NetBoot HD" by default. If the computers in a list use NetBoot, you should make sure the hard disk name is the same for NetBoot and non-Netboot computers. This ensures that the paths to all applications used on these clients are the same.

To use a specific hard disk name:

1 In Macintosh Manager, click Computers, and then click Control.

2 Select a computer list, then select "Force computer hard disk name to __" and type in the name you want to use (for example, Macintosh HD).

3 Click Save.

If you have difficulty using Macintosh Manager to specify a hard disk name for computers, make sure file sharing is turned off on the client computers.

To turn off file sharing, use the File Sharing control panel.

Creating Email Addresses for Managed Users

Macintosh Manager can create an email address for a user who doesn't already have one. When a user logs in, Macintosh Manager adds the user's short name to the default domain name you specify and creates an email address.

If a user has other imported email settings, they will override Macintosh Manager's settings when the user connects to the Macintosh Manager network.

To create an email address for a user:

1 In Macintosh Manager, click Computers, and then click Control.

2 Select a computer list.

3 Under User Email Addresses, type the default domain name, the incoming (POP) mail server address, and the outgoing (SMTP) server address.

4 Click Save.

To have the computer check for messages when the user logs in, select "Check for email when members log in" in the Options pane of the Workgroups pane.

Using Security Settings for Computers

Computer security settings let you choose security settings for users, computers, and applications.

Keeping Computers Secure If a User Forgets to Log Out

If a user doesn't log out when he or she finishes using a computer, other people can use the computer without logging in. They will have access to anything the previous user had access to, including that user's home directory and documents. You can prevent this type of unauthorized access with the idle logout feature.

Idle logout occurs when there is no user activity (such as typing or using the mouse) for a specified period of time. For example, suppose you enable idle logout after 15 minutes. A user logs in, works for a while, and then decides to leave the computer and go have a snack, but doesn't log out. After 15 minutes, the user returns and must enter a user name and password again to gain access.

To enable idle logout:

1. In Macintosh Manager, click Computers, and then click Control.
2. Select a computer list, then select "Enable idle log-out" and enter the number of minutes the computer should wait.
3. Choose a logout option.

   If you select "Log user out," users see a dialog after idle logout and have the opportunity to save any unsaved documents, and then they return to the login screen.

   If you select "Lock the screen," the screen goes black and a dialog appears. Users can save any unsaved documents, and then they can either enter a password and continue working or log out.
4. Click Save.

   If this feature has been activated and the computer is connected to the network, you can use a Mac OS X Server administrator password to log in.

Allowing Access to All CDs and DVDs

Using computer security settings, you can allow user access to CDs and DVDs with no restrictions.

To allow access to any CD or DVD:

1. In Macintosh Manager, click Computers.
2. Click Security and select a computer list.
3. Select "Access all CD-ROMs" and click Save.
4. Select "Show a panel for inserted CD-ROMs" to make it easy for Panels workgroups to find inserted CDs.

Allowing Access to Specific CDs or DVDs

You can restrict user access to CDs and DVDs by using a list of approved discs. You can also allow users to access only certain files on a CD or DVD.

First, create the list of approved discs and items, and then allow user access to the discs.

To allow access to only specific CDs or DVDs:

1 In Macintosh Manager, make sure you have already set up a list of approved discs and items in the CD-ROMs pane of the Global pane.

See "Using Global CD-ROM Settings" on page 226 for instructions.

2 Click Computers, then click Security and select a computer list.

3 Select "Access approved CD-ROMs only."

4 Select "Show a panel for inserted CD-ROMs" to make it easy for Panels workgroups to find inserted CDs.

Choosing Computer Security Settings for Applications

Some applications may occasionally use "helper applications" to do jobs they cannot do themselves. For example, if a user clicks a web link in an email message, the email application might want to open a web browser. Other applications, such as installers, may need to quit the Finder and restart in order to finish their jobs.

Important: Macintosh Manager doesn't automatically allow these options, but you may choose to do so. Allowing these options can weaken computer security.

To allow applications to open other applications or quit the Finder:

1 In Macintosh Manager, click Computers, and then click Security and select a computer list.

2 Select "Open other applications, such as helper applications" and/or select "Quit the Finder" to allow these options for applications.

3 Click Save.

Allowing Specific Applications to Be Opened by Other Applications

You can allow specific applications to act as helper applications for other applications that might need to use them. The applications you want to designate as helpers must already be added to the list of allowed items for one or more workgroups.

To specify helper applications:

1 Open Macintosh Manager.

2 Choose Application Preferences from the Configure menu.

3 Select an application in the list.

The list only shows applications currently assigned to workgroups. If the application you want isn't in the list, click Add to browse for the application, or click Custom and type the name and four-character code of the application you want to add.

4 To designate the application as a valid helper, select "Allow this application to be opened by other applications."

Allowing Users to Work Offline

If the Macintosh Manager server or a user's home directory is not available, you can still allow offline computer use. The user must log in, but the Macintosh Manager server is not available. If the home directory is not available, users may not be able to save their documents.

To allow users to work offline:

1 In Macintosh Manager, click Computers.

2 Click Security and select a computer list.

3 Select "Work offline if the Macintosh Manager Server is not available" to allow this option for users. If you want, you can also select "Require an Administrator password to work offline" for this option.

4 Select "Work offline if the user's home directory is not available" to allow this option for users.

5 Click Save.

Switching to a Different Macintosh Manager Server

To change servers from the Macintosh Manager administrator application, choose Change Server from the File menu. Regular users can click Change Server in Macintosh Manager's dialog at login and switch to a new Macintosh Manager server using an administrator password. Either way, be sure to select Local (or Local Network) in the Select Macintosh Management Server dialog, and then select the server you want to use.

Note: If your network doesn't use AppleTalk, you may not see a Local or Local Network section. In that case, simply select the server you want to use from the list of available servers.

If you wish, you can allow users to switch to a different server without requiring an administrator password by following the steps below.

Important: Allowing this option can decrease server security. Also, if you have servers that use older versions of Macintosh Manager, switching a client computer to one of these servers may cause the server to install the older software on the client computer.

To allow users to switch servers without using a password:

1 In Macintosh Manager, click Computers.

2 Click Security and select a computer list.

3 Select "Switch to another server without authentication" to allow this option for users.

4 Click Save.

If you want NetBoot client computers to choose a different Macintosh Manager server, remove the DNSPlugin extension from the NetBoot image.

Allowing Users to Force-Quit Applications

If you allow users to force-quit applications, they can press Command-Option-Esc to force an application to quit.

Note: Allowing this option may pose a security risk.

To allow users to force-quit:

1 In Macintosh Manager, click Computers.

2 Click Security and select a computer list.

3 Select "Force Quit applications" to allow this option for users.

4 Click Save.

Allowing Users to Disable Extensions

If users are allowed to restart computers, you can also allow them to turn off extensions by pressing the Shift key during startup. This will not disable the Macintosh Manager extension or necessary system extensions.

Note: Allowing this option may pose a security risk.

To allow users to start up with extensions off:

1 In Macintosh Manager, click Computers.

2 Click Security and select a computer list.

3 Select "Disable extensions during startup" to allow this option for users.

4 Click Save.

Using Computer Login Settings

Computer login settings allow you to choose how users log in, what messages they see, and what panel names look like.

Choosing How Users Log In

When users log in to a computer, they can either type their names or choose their names from a list. If you decide to use a list for login, the list can contain up to 2000 users. You can choose not to display administrators in that list.

To set login options:

1 In Macintosh Manager, click Computers.

2 Click Log-In and select a computer list.

3 Select "Users choose their name from a list (1-2000 users)" to use the list option. If you don't want administrator names to appear in the list, select "List displays users only (no administrators)."

4 If you don't want to use a list, select "Users type their name."

5 Click Save.

Creating Login Messages for Computers

You can create two types of messages for computers. Each can contain up to 127 characters.

- The banner message appears in the login dialog.
- The server message appears in a separate panel after users log in. It is preceded by the phrase "From: Global Administrator."

To set up a login message:

1 In Macintosh Manager, click Computers.

2 Click Log-In and select a computer list.

3 Type your banner message or server message in the appropriate message text box.

If you don't want to use a message, leave the text box blank.

4 Click Save.

Customizing Panel Names

You can customize the names of the workgroup and user documents panels shown for Panels workgroups.

To customize a panel name:

1 In Macintosh Manager, click Computers.

2 Click Log-In and select a computer list.

3 If you want the workgroup's name to appear on a workgroup documents panel, select "Show the workgroups name" or click the button next to the text box and type a different name.

4 If you want the user's name to appear on a user document panel, select "Show the user's name" or click the button next to the text box and type a different name.

5 Click Save.

Managing Portable Computers

It is important to plan how you want to manage portable computers that have access to your network. This section gives suggestions for managing portable computers and tells you how to use Macintosh Manager's checkout feature.

Portable Computers With Network Users

You can let users share specific portable computers, such as those in an iBook Wireless Mobile Lab. An iBook Wireless Mobile Lab contains either 10 or 15 student iBooks (plus an additional iBook for an instructor), an AirPort Base Station, and a printer, all on a mobile cart. The cart lets you take the computers to your users (for example, from one classroom to another).

To manage the mobile lab, first create a computer list containing all of the iBooks. Make sure users have network accounts and home directories, and then assign sets of users to workgroups that will use the iBooks. You might want to create different workgroups for different purposes, such as one for a history class, one for a biology class, and so on. You can use the Check Out feature to allow these workgroups to use the iBooks.

You can use the All Other Computers account to manage network users who have their own portable computers. See "Providing Quick Access to Unimported Users" on page 191 for more information.

Portable Computers With Local Users

Local user accounts cannot be managed using Macintosh Manager. However, you can use the Multiple Users control panel to set up local user accounts on specific computers in one of two ways:

- The user doesn't have administrator privileges, but has a local account.
- The user is the administrator for the computer.

If the user is the local administrator, he or she has total access to the all folders and applications on the computer, including the System Folder.

Letting Users Check Out Computers

You can allow users to check out and take home a portable computer (to continue working on a project after school, for example). Macintosh Manager settings and security features remain in effect on the computer even while it is checked out.

To check out a computer:

1 In Macintosh Manager, click Computers.

2 Click Check Out and select a computer list.

3 Select "These computers can be Checked Out" and then select one of the checkout options in the steps that follow.

4 Select "All users are allowed to Check Out these computers" to allow this option.

5 Select "Allow only the following users to Check Out these computers" to restrict checkout to a list of specific users. Then, select users in the Available Users list and click Add to make them allowed users.

To remove users from the Allowed user list, select one or more users and click Remove.

6 Click Save.

Using Wireless Services

You can provide wireless network service to managed clients using AirPort, for example. Make sure the Macintosh Manager Server is within range of your wireless service. If a user on a portable computer goes out of range, he or she cannot log in to Macintosh Manager, but you can allow the user to work offline. See "Allowing Users to Work Offline" on page 220 for more information.

Wireless connections may have a slower data transfer speed than a direct connection (such as an ethernet cable). If you need more information about using AirPort, consult AirPort documentation or visit the website: www.apple.com/airport/.

Using Global Security Settings

In Macintosh Manager, global security settings apply to your entire Macintosh Manager network (all users, groups, and computers). These settings cover a variety of options that affect reports, guest access, passwords, and how preferences are copied.

Using Macintosh Manager Reports

Macintosh Manager provides a number of different reports to help you keep track of user and network activity.

To view a report:

1 Open Macintosh Manager.

2 Choose the report you want from the Report menu.

You can view the selected report immediately, and then export it to a file or print it if you wish.

You can set additional criteria for the Activity Log report and the Computers report before you see the results.

Setting the Number of Items in a Report

You can set the maximum number of log entries to show in Macintosh Manager reports.

Note: The Connected Users report will show only up to 300 log entries, even if the maximum number of log entries you set is greater than 300.

To set how many log entries are tracked:

1 In Macintosh Manager, click Global, and then click Security.

2 In the text box next to "Maximum number of log entries," type a number.

To view a report, go to the Report menu and choose the report you want to see.

Keeping the Administration Program Secure

If an administrator forgets to quit the Macintosh Manager administration application, another person could potentially make changes and save them. To prevent this kind of unauthorized access, you can make the administration application quit after a specified time if there is no user activity.

> *Warning:* When the administration application quits automatically, unsaved changes are lost.

To allow the administration program to quit automatically:

1 In Macintosh Manager, click Global, and then click Security.

2 Select "Quit the administration program if idle for __ minutes" and enter the number of minutes the application should wait before quitting automatically.

3 Click Save.

Verifying Login Information Using Kerberos

If all users must authenticate using Kerberos, follow the steps below. For more information about using Kerberos, see the Open Directory administration guide.

To use Kerberos verification:

1 In Macintosh Manager, click Global, and then click Security.

2 Select "Clients must authenticate using Kerberos" and click Save.

Managing User Passwords

Ordinarily, all users can change the passwords assigned to them. If you don't want users to change their own passwords, you can remove that privilege.

To keep users from changing their passwords:

1. In Macintosh Manager, click Global, and then click Security.
2. If "Users can change their passwords" is selected, deselect it.
3. Click Save.

Allowing Administrators to Access User Accounts

You can allow a system administrator to log in as any user. The user can enter the user name for the account he or she wants to access and use the appropriate administrator password.

To allow administrators to log in as other users:

1. In Macintosh Manager, click Global, and then click Security.
2. Select "Users may log in using a server administrator's password."
3. Click Save.

Using Global CD-ROM Settings

Global CD-ROM settings let you allow access to all CDs and DVDs or to only a specific list of discs. When you make a disc available to Macintosh Manager, you can view its contents, and then you can allow users access to all items on the disk or just the items you select.

Note: These settings don't apply to audio CDs. The audio CD setting is in the Privileges pane of the Workgroups pane.

To create a list of available discs and disc items:

1. In Macintosh Manager, click Global, and then click CD-ROMs.
2. Insert a CD or DVD.
3. Select the disc name and click Add to make it available in Macintosh Manager. To remove an available item, select it and click Remove.
4. To make specific items on a disc available to users, select a CD or DVD in the "Available in Macintosh Manager" list.

   In the "Allowed items on (__)" list, select items you want to make available to users. Click Allow All to select and allow every item on the disc. Click Allow None to deselect all items.
5. When you have finished, click Save.

To make only your list of approved items available to users, select a computer list and make sure to select "Access approved CD-ROMs only" in the Security pane for Computers. You may also want to select "Show a panel for inserted CD-ROMs" to make it easy for Panels workgroups to find inserted CDs.

Managing Preferences

You can use the Managed Preferences folder to customize how application preferences and system preferences are handled to meet your particular needs and goals. For example, you can make sure that users always start out with a specific set of preferences or that some user-set preferences are never overridden.

A Managed Preferences folder is created on the workgroup data volume the first time any member of a workgroup logs in. Inside this folder are two (initially empty) additional preference folders, the Initial Preferences folder and the Forced Preferences folder.

Using Initial Preferences

Preferences in the Initial Preferences folder are set once during login. The first time users log in, they get a fresh copy of any preferences contained in the Initial Preferences folder. Users can modify these preferences, and the changes are saved at logout.

For example, in a classroom setting, a teacher can set up preferences and a list of bookmarks for a particular web browser. He or she stores a copy of those preferences in the Initial Preferences folder. When students log in on the first day of class, they all start out with the same browser preferences and the same list of bookmarks.

After a user's first login, Macintosh Manager checks the user's Preferences folder and compares it to the contents of the Initial Preferences folder. If a user already has a preference in the folder, Macintosh Manager doesn't replace that preference. If a user's folder doesn't contain one or more initial preferences, Macintosh Manager copies the missing files to the user's folder.

This process is repeated each time a user logs in, so you can place additional preference files in the Initial Preferences folder later. For example, if you install new software and place the software preferences file in the Initial Preferences folder, Macintosh Manager copies the new file to a user's Preferences folder when the user opens the new software for the first time.

To use the Initial Preferences folder:

1 Set up a workgroup data volume (Group Documents) in the Options pane of the Workgroups pane.

2 From a client computer, access the group documents volume.

3. Create any preferences you want to place in the Initial Preferences folder.
4. Copy the preferences you created to the Initial Preferences folder on the group documents volume.
5. In the Finder, select the Initial Preferences folder and press Command-I to open the Show Info window.
6. Choose Sharing from the Show pop-up menu.
7. Select "Share this item and its contents" and make sure the privileges are correct.
8. Click Copy to apply the privileges to all enclosed folders.
9. Repeat steps 1 through 4 for each group documents volume.

Certain preferences don't need to be included in the Initial Preferences folder. See the administrator's guide for more details.

Exceptions to Initial Preferences

A few preferences are created automatically the first time a user logs in, regardless of whether you're using an Initial Preferences folder. You don't need these items in the Initial Preferences folder because they won't be copied to the user's folder:

- Apple Menu Options Preferences
- AppSwitcher Preferences
- Internet Preferences
- Keyboard Preferences
- Keychains
- Location Manager Preferences
- Mac OS Preferences
- TSM Preferences
- User Preferences

Using Forced Preferences

Using the Forced Preferences folder lets you ensure that users start out with a specified set of preferences every time they log in. If a user changes his or her preferences, those preferences are replaced with the preferences in the Forced Preferences folder the next time the user logs in.

When a user logs in on a Mac OS 9 computer, Macintosh Manager compares preference folders and files in the /Library/Classic folder of a user's home directory to items in the Forced Preferences folder. Macintosh Manager deletes any matching items from the user's folder and replaces them with preferences from the Forced Preferences folder. If any forced preferences are missing from the user's folder, Macintosh Manager places new copies of these items in the user's Preferences folder.

If there are items in the user's Preferences folder that don't match any items in the Forced Preferences folder, Macintosh Manager does nothing to them. If you have concerns about these items accumulating or consuming disk space, clean out the user's Preferences folder occasionally.

To use forced preferences:

1 Set up a workgroup data volume (Group Documents) in the Options pane of the Workgroups pane.

2 From a client computer, access the group documents volume.

3 Create any preferences you want to place in the Forced Preferences folder.

4 Copy the preferences you created to the Forced Preferences folder on the group documents volume.

5 In the Finder, select the Forced Preferences folder and press Command-I to open the Show Info window.

6 Choose Sharing from the Show pop-up menu.

7 Select "Share this item and its contents" and make sure the privileges are correct.

8 Click Copy to apply the privileges to all enclosed folders.

9 Repeat steps 1 through 4 for each group documents volume.

Sharing Mac OS 9 Application Preferences in the Classic Environment

You can use Workgroup Manager to make sure preferences for Mac OS 9 applications are maintained when the application is opened in Mac OS X using the Classic environment. This way, users with network home directories will keep the same Mac OS 9 application preferences when they log in on different computers. This also ensures that Mac OS 9 application preferences are preserved when a managed user switches from a Macintosh Manager client computer (using Mac OS 9) to a Workgroup Manager client computer (using Mac OS X).

To share preferences with Classic:

1 From your administrator computer, open Workgroup Manager.

2 Make sure the right directory is selected and that you are authenticated for it.

To switch directories, click the small globe above the accounts list. If you are not authenticated, click the lock.

3 Select an account, then click Preferences.

4 Click Classic, then click Advanced.

5 Set preference management to Always.

6 Select "Use preferences from home folder."

7 Click Apply Now.

Alternatively, you can do the following on each Mac OS X client. Open System Preferences, click Classic, then click Advanced and select "Use preferences from home folder."

Where to Find More Information

The AppleCare website provides a variety of resources, including the Knowledge Base (a database containing technical articles about product usage, implementation, and problem solving). Investigate the website at www.apple.com/support.

Discussion lists for Mac OS X Server and Macintosh Manager let you exchange ideas and tips with other server administrators. You can sign up for a discussion list at www.lists.apple.com.

Solving Problems

11

If you encounter problems as you work with Workgroup Manager or Macintosh Manager, you may find a solution in this chapter.

Online Help and the Apple Knowledge Base

If the answer to your question isn't here, try searching Mac OS X Server online Help for new topics. You can also search the Apple Knowledge Base for information and solutions: www.info.apple.com.

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).

You Can't See Certain Users in the Login Window

When you upgrade to Mac OS X version 10.3 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 users with user IDs smaller than 500, but they can still log in by entering a user name and password.

To set up a Mac OS X computer's login window to show network users:

1. Set up a shared directory on Mac OS X Server.
2. In Workgroup Manager, click Accounts.
3. Select a computer list that resides in the shared directory.

4 Select "Define Guest computer preferences here," and click Save.

5 Click Preferences, click Login, and click Login Options.

6 Select "List of users able to use these computers" and "Show network users." Click Apply Now.

7 Configure a Mac OS X version 10.3 computer associated with the computer list to use the shared directory.

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/root, 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. Select the user's account (or create a new account for the user) in a directory domain on that server, and select "User can administer the server" on the Basic pane.

Users Can’t Log In or Authenticate

Try these techniques to determine whether the source of the authentication problem is configuration or the password itself:

- Reset the password to a known value, then determine whether there is still a problem. Try using a 7-bit ASCII password, which is supported by most clients.
- Make sure that the password contains characters supported by the authentication protocol. Leading, embedded, and trailing spaces as well as special characters (for example, Option-8) are not supported by some protocols. For example, leading spaces work over POP or AFP, but not over IMAP.
- Make sure that the user’s current keyboard can generate all the characters in the user’s password.
- Basic authentication doesn’t support many authentication methods. To increase the possibility that a user’s client applications will be supported, set the user’s password type to Open Directory or suggest that the user try a different application.
- If user’s account resides in a directory domain that is not available, you can create a user account in a directory domain that is available.
- 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 of the Open Directory Password Server’s authentication methods, such as APOP or CRAM-MD5, then the user’s applications will be unable to authenticate with the disabled methods. The Open Directory administration guide explains how to disable and enable authentication methods with a command-line tool. After enabling or disabling Open Directory Password Server authentication methods, you may need to reset the user’s password.
- For Kerberos troubleshooting tips, see “Users Can’t Authenticate Using Single Signon or Kerberos” on page 235.
- If a Mac OS 8.1–8.6 computer fails to authenticate for Apple file service, the computer’s AppleShare Client software may need upgrading.
  - Mac OS 8.6 computers should use AppleShare Client version 3.8.8.
  - Mac OS 8.1–8.5 clients should use AppleShare Client version 3.8.6.
  - Mac OS 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 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 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 Directories

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

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 on the Accounts pane of System Preferences.

A Mac OS X User in Shared NetInfo Domain Can't Log In

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

Users Can't Authenticate Using Single Signon or Kerberos

When a user or service that uses Kerberos experiences authentication failures, try these remedies:

- Kerberos authentication is based on encrypted time stamps. If there's more than a five-minute difference between the KDC, client, and service computers, authentication may fail. Make sure that the clocks for all computers are synchronized using the Network Time Protocol (NTP) service of Mac OS X Server or another network time server. For information about the NTP service of Mac OS X Server, see the network services administration guide.
- Make sure that Kerberos authentication is enabled for the service in question.
- If a Kerberos server used for password validation is not available, reset the user's password to use a server that is available.
- Make sure that the server providing the Kerberized service has access to directory domains containing accounts for users who are authenticated using Kerberos. AFP, mail, and other Kerberized services of Mac OS X Server always have access to user accounts in the server's local directory domain and its LDAP directory domain, if it has one. For information about configuring access to directory domains on other servers, see the Open Directory administration guide.
- Refer to the KDC log (kdc.log) for information that can help you solve problems. Incorrect setup information such as wrong configuration file names can be detected using the logs.
- Make sure all Kerberos configuration files are complete and correct. For example, make sure the keytab file on your server has the principals of interest in it.
- If users can't authenticate using single signon or Kerberos for services provided by a server that is joined to an Open Directory master's Kerberos domain, the server's computer record might be incorrectly configured in the Open Directory master's LDAP directory. In particular, the server's name in the computer list must be the server's fully qualified DNS name, not just the server's host name. For example, the name could be server2.example.com but not just server2.

To reconfigure a server's computer record for single signon and Kerberos authentication:

1 Delete the server from the computer list in the LDAP directory.

2 Add the server to the computer list again.

3 Delegate authority again for joining the server to the Open Directory master's Kerberos domain.

4 Rejoin the server to the Open Directory master for single signon and Kerberos authentication.

For detailed instructions, see "Adding Computers to an Existing Computer List" on page 96, "Deleting Computers From a Computer List" on page 97, and 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 AppleCare Knowledge Base online.

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 client computer's email application's own preference settings 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 include it in the Guest Computers list.

If a user with a local account doesn't see a list of workgroups at login:

- The user's computer may not have any workgroups assigned to it. Assign one or more groups to the computer list (or Guest Computers list) to which that computer belongs.
- The user's computer may not be in a computer list. Add the computer to a computer list or include it in the Guest Computers list.

Users Can’t Open Files

Ordinarily, users can double-click a file in the Finder or select a file and choose Open from the Finder’s File menu, and then an appropriate default application will open 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 will 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 in the Items pane of the Applications preference.

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 add printers to 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 additional printers available to specific users, groups, or lists of computers using the Printer List pane of Printer preferences.

Note: If “Allow user to add printers to 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.

A user can add additional login items if allowed to do so. However, if you select Once as the management setting for Login Items, any items the user added will be removed the next time the user logs in. Afterward, the user may add additional login items if allowed to do so.

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.

A user can add additional items to his or her Dock if allowed to do so. However, if you select Once as the management setting for Dock Items, any items the user added will be removed the first time the user logs in. Afterward, users may still place additional items in the Dock if allowed to do so.

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, then re-specifying 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 the original items are located on a remote server and the user is not connected to that server, the corresponding Dock items will appear as question mark icons.

A user can click a question mark icon to reconnect to a server (the server prompts the user for a password if needed). Once connected to the server containing the original items, the user's Dock icons will return to normal and open the appropriate item when clicked.

Users See a Message About an Unexpected Error

When you manage Classic preferences and try to use the Extensions Manager, File Sharing, and 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.

Solving Macintosh Manager Problems

This section describes some problems you may encounter while using Macintosh Manager and provides troubleshooting tips and possible solutions. If your problem is not addressed here, you may want to check Macintosh Manager Help or consult the AppleCare Knowledge Base online.

I've Forgotten My Administrator Password

Contact your Mac OS X Server administrator if you forget your password. If necessary, the server administrator can change your password using the Workgroup Manager application.

Administrators Can't Get to the Finder After Logging In

If you have system access, you can choose the System Access workgroup when you log in. If you don't have system access, and you need to go to the Finder often, ask your Macintosh Manager administrator to enable system access for your account.

You can bypass Macintosh Manager login by pressing Command-Shift-Esc when the Welcome dialog appears. Then enter either the computer owner's password or a local administrator's name and password.

Generic Icons Appear in the Items Pane

If generic icons appear in the Items pane of the Workgroups pane in Macintosh Manager, restart the computer with Mac OS 9 and rebuild the Desktop file.

Selecting "Local User" in the Multiple Users Control Panel Doesn't Work

You cannot use both Macintosh Manager client software and the Multiple Users control panel on the same computer.

If you want to set up local users, don't install Macintosh Manager client software on the computer. Instead, install the Multi-User Startup extension and use the Multiple Users control panel version 1.4.1.

Some Printers Don't Appear in the Available Printers List

When you make printers available to client computers, Macintosh Manager creates desktop printers for your Mac OS 9 clients. The Mac OS X version of the Macintosh Manager administrator application creates only LaserWriter desktop printers. If you need to provide access to non-LaserWriter printers, you must use the Mac OS 9 version of the Macintosh Manager administrator application to manage clients.

Users Can't Log In to the Macintosh Manager Server

First, make sure the server has enough free disk space. If the user's password has not been changed and his or her user account has not been deleted, check the user's Macintosh Manager login privileges.

To make sure login is enabled:

1. In Macintosh Manager, click Users, and then click Basic.
2. Make sure "User can log in" is selected. If "Disable login as of __" is also selected, make sure the date has not already passed.

Users Can't Log In as "Guest" on Japanese-Language Computers

If users need to log in using the Guest account on Japanese-language client computers, you must change the computer's language script to Roman in the International pane of System Preferences.

A Client Computer Can't Connect to the Server

Try doing the following:

- Make sure the server is running. If you recently started the server, it may take a few minutes for the server to appear.
- Make sure network information (including DNS information) is entered correctly.
- Make sure the client computer is not low on memory and that it is connected to the network.
- If many computers start up at once, the load on your network may be too great. Try starting fewer computers at one time.

The Server Doesn't Appear in the AppleTalk List

Mac OS X Server doesn't support AppleTalk network connections to Apple Filing Protocol (AFP) servers, such as the Macintosh Manager server. To connect to AFP servers, set client computers to connect via TCP/IP.

Macintosh Manager client computers can, however, use AppleTalk for service discovery. If your network has AppleTalk zones, users on Mac OS 8 computers may need to select the zone where the server resides. On Mac OS 9 computers, use the Network Browser to make sure you're connected to the server.

The User's Computer Freezes

If the computer's system software is earlier than Mac OS 9, be sure file sharing is turned off.

Users Can't Access Their Home Directories

Users may see a message if their home directories cannot be found at login.

In Workgroup Manager, make sure the user's home directory exists and has the correct permissions settings. Then, make sure the server that contains the user's home directory is connected.

Users Can’t Access Shared Files

Shared workgroup folders are normally located on the same server volume. However, if you store workgroup documents on more than one volume, some users may not be able to access all of their shared documents without changing workgroups.

If the user belongs to more than one workgroup and workgroup documents are stored on several servers, make sure the user has the latest version of AppleShare.

When a Macintosh Manager client computer is connected to a server that uses Mac OS X version 10.2, users cannot access shared folders, such as the Groups Folder or Shared Documents folder, located on that server.

To be certain users have access to those shared folders, store the folders on a different server.

Shared Workgroup Documents Don’t Appear in a Panels Environment

If you created a workgroup data volume but users in a Panels workgroup can’t see it, make sure the workgroup data volume contains the shared documents folders.

Also check to make sure the location of the Users folder has not changed. The Users folder is usually located at the top level of either the server volume or the workgroup data volume.

Applications Don’t Work Properly or Don’t Open

Some applications write to or create special files in places other than the Preferences folder inside the System Folder. If you enforce file-level security for a workgroup, some older applications may not function properly or may report errors. See “Preventing Applications From Altering Files” on page 202 for more information.

You can create a folder called “Other Applications” and then put the Applications folder (and all of its contents) inside. The Other Applications• folder must reside in the client computer’s Applications folder. If the client computer is running Mac OS 9.1 or later, the Applications folder is called “Applications (Mac OS 9).”

Users Can’t Drag and Drop Between Applications

In most cases, Macintosh Manager doesn’t allow the drag-and-drop feature. Use the Copy and Paste commands instead.

Users Can’t Open Files From a Web Page

Sometimes web browsers rely on helper applications to open files that the browser itself cannot handle (for example, media files or PDF files).

1. In Macintosh Manager, click Computers, and then click Security.
2. Select “Open applications, such as helper applications.”

Sometimes the Right Application Doesn’t Open for Users

If the wrong application opens when a user tries to open a document, try rebuilding the client computer’s desktop.

Importing and Exporting Account Information

This appendix provides guidelines for importing and exporting account information.

Several tools—Workgroup Manager and `dsimport`—are available to help you export and import accounts.

Understanding What You Can Import

You can import and export account information from a data file using Workgroup Manager. You can also use the `dsimport` tool.

Note: You will need to reset the password for user accounts whose password type is Open Directory.

The user and group account attributes you can import vary with the kind of import file:

- XML files created with Mac OS X Server 10.1 or earlier
- XML files created with AppleShare IP 6.3
- Character-delimited files

You cannot use an import file to change these predefined users: daemon, root, nobody, unknown, or www. Nor can you use an import file to change these predefined groups: admin, bin, daemon, dialer, mail, network, nobody, nogroup, operator, staff, sys, tty unknown, utmp, uucp, wheel, or www. You can, however, add users to the wheel and admin groups.

Importing and Exporting Information for Macintosh Manager

For information about importing and exporting information for users and groups on Mac OS 9 clients, read Chapter 10, "Using Macintosh Manager for Mac OS 9."

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.

To import accounts using Workgroup Manager:

1 Create a character-delimited or XML file containing the accounts to import, and place it in a location accessible from the server on which you will use Workgroup Manager. The LDAP directory of an Open Directory master supports up to 100,000 records. For local NetInfo databases, ensure the file contains no more than 10,000 records.

See "Using XML Files Created With Mac OS X Server 10.1 or Earlier" on page 245, "Using XML Files Created With AppleShare IP 6.3" on page 246, and "Using Character-Delimited Files" on page 247 for information on creating files to import.

2 In Workgroup Manager, click Accounts, then click the globe icon below the toolbar and choose the directory domain into which you want to import accounts.

3 Click the lock to authenticate as domain administrator.

4 Choose Import from the Server menu, then select the import file.

5 Select one of the Duplicate Handling options to indicate what to do when the short name of an account being imported matches that of an existing account.

"Overwrite existing record" overwrites any existing record in the directory domain.

"Ignore new record" ignores an account in the import file.

"Add to empty fields" merges data from the import file into the existing account when the data is for an attribute that currently has no value.

"Append to existing record" appends data to existing data for a particular 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.

6 Define a user account preset in the server's LDAP directory.

The settings you associate with a preset are assigned to each imported user, simplifying the definition of user profile path, login script, home directory share point, and other values.

7 Click New User and specify values you want all imported users to inherit.

8 Set up password options so that users are forced to change their passwords the next time they log in.

This approach means you don't have to specify individual passwords for each user in the export file or in Workgroup Manager after importing the users. To access password option settings, click Advanced, then Options.

9 When you are finished specifying values, choose Save Preset from the Presets pop-up menu.

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

10 In the First User ID field, enter the user ID at which to begin assigning user IDs to new user accounts for which the import file contains no user ID.

11 In the Primary Group ID field, enter the group ID to assign to new user accounts for which the import file contains no primary group ID.

12 Click Import to start the import operation.

Using Workgroup Manager to Export Users and Groups

You can use Workgroup Manager to export user and group accounts from 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, then click the globe icon below the toolbar and choose the directory domain from which you want to export accounts.

2 Click the lock to authenticate as domain administrator.

3 Click the Users button to export users or the Groups button to export groups.

4 To export all accounts listed, select all of them. To export a specific account, select it. To export multiple accounts, select them while holding down the Command or Shift key.

5 Choose Export from the Server menu.

6 Specify the name to assign to the export file and the location where you want it created.

7 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. For instructions, see the command-line administration guide.

Using XML Files Created With Mac OS X Server 10.1 or Earlier

You can use Server Admin to create an export file from Mac OS X Server versions 10.1 or earlier, and import that file into 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. Attributes in angle brackets (<>) are required and will generate an error if absent when you use the file as an import file:

- indication of whether user can log in
- indication of whether user is a server administrator
- <User ID>
- <primary group ID>
- shell
- comment
- <short name>
- <long name>
- <password format> and <password text>
- Apple mail data
- ara (Apple Remote Access; this data is ignored)

The following group account attributes might be present in these XML files:

- <group name>
- <group ID>
- <one member's short name>
- other members' short names

Using XML Files Created With AppleShare IP 6.3

You can use the Web & File Admin application to create an export file on an AppleShare IP 6.3 server and import that file into 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. Attributes in angle brackets (<>) are required and will generate an error if absent when you use the file as an import file:

- <name> (mapped to a long name)
- inetAlias (mapped to a short name)
- comment
- indication of whether user can log in
- <password format> and <password text>
- Apple mail data
- indicator for whether the user is a server administrator, password change data, and indicator for forcing a password to change (this data is ignored)

The 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>
- <one member's short name>
- other members' short names

dsimport 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 create a character-delimited file by using Workgroup Manager or dsimport to export accounts in the LDAP directory of an Open Directory master or a NetInfo domain into a file. You can also create a character-delimited file by hand or by using a database or spreadsheet application.

The first record in the file must characterize the format of each account in the file. There are three options:

- Write a full record description.
- Use the shorthand "StandardUserRecord."
- Use the shorthand "StandardGroupRecord."

The other records in the file describe user or group accounts, encoded in the format described by the first record.

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; and it describes the escape character that precedes special characters in a record. Encode the record description using the following elements in the order specified, separating them using a space:

- End-of-record indicator (in hex notation)
- Escape character (in hex notation)
- Field separator (in hex notation)
- Value separator (in hex notation)
- Type of accounts in the file (DSRecTypeStandard:Users or DSRecTypeStandard:Groups)
- Number of attributes per account
- List of attributes

For user accounts, the list of attributes must include the following:

- RecordName (the user's short name)
- RealName (the user's long name)
- NFSHomeDirectory
- Password
- UniqueID (the User ID)*
- PrimaryGroupID*

*You can omit these if you specify a starting user ID and a default primary group ID when you import the file.

In addition, you can include

- UserShell (the default shell)
- NFSHomeDirectory (the path to the user's home directory on the user's computer)
- Other user 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

Here is an example of a record description:

```
0x0A 0x5C 0x3A 0x2C DSRecTypeStandard:Users 7
RecordName Password UniqueID PrimaryGroupID
RealName NFSHomeDirectory UserShell
```

Here is an example of a record encoded using the description:

```
jim:Adl47E$:408:20:J. Smith, Jr., M.D.:/Network/Servers/somemac/
     Homes/jim:/bin/csh
```

The record consists of values, delimited by colons. Use a double colon (::) to indicate a value is missing.

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 will be 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 "password"):

```
dsAuthMethodStandard\:dsAuthClearText:password
```

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 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 use the Password Server. It must be typed as one line of text in which the elements are separated by spaces and without line breaks, as presented here. Although your browser will wrap the text for presentation, you can see that it contains no line breaks if you copy and paste it into a text editor that has wrapping turned off:

```
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: password1
Unique ID: 1242
Primary Group ID: 20
Comment: <blank>
Real Name (long name): Terri User
User Shell: /bin/tcsh
tuser:dsAuthMethodStandard\:dsAuthClearText:password1:1242:20::Tom
     User:/bin/tcsh
```

Note: This example also uses the colon (:) as the field separator and the backslash (\) as the escape character.

As these examples illustrate, you can use the prefix `dsAttrTypeStandard:` when referring to an attribute, or you can omit the prefix. When you use Workgroup Manager to export character-delimited files, it uses the prefix in the generated file.

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.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined "admin" group.

administrator computer A Mac OS X computer onto which you have installed the server 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.

authentication authority attribute A value that identifies the password validation scheme specified for a user and provides additional information as required.

BIND (Berkeley Internet Name Domain) The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

boot ROM Low-level instructions used by a computer in the first stages of starting up.

BSD (Berkeley System Distribution) A version of UNIX on which Mac OS X software is based.

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

CGI (Common Gateway Interface) A script or program that adds dynamic functions to a website. A CGI sends information back and forth between a website and an application that provides a service for the site. For example, if a user fills out a form on the site, a CGI could send the message to an application that processes the data and sends a response back to the user.

child A computer that gets configuration information from the shared directory domain of a *parent*.

computer account 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 distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a *lease period*—the length of time the client computer may use the address.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a directory node or simply a directory.

directory domain hierarchy A way of organizing local and shared directory domains. A hierarchy has an inverted tree structure, with a root domain at the top and local domains at the bottom.

directory node See *directory domain.*

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

disk image A file that when opened (using Disk Copy) creates an icon on a Mac OS desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software.

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

drop box A shared folder with privileges that allow other users to write to, but not read, the folder's contents. Only the *owner* has full access. Drop boxes should only be created using AFP. When a folder is shared using AFP, the ownership of an item written to the folder is automatically transferred to the owner of the folder, thus giving the owner of a drop box full access to and control over items put into it.

dynamic IP address An IP address that is assigned for a limited period of time or until the client computer no longer needs the IP address.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a website visitor.

export The Network File System (NFS) term for sharing.

filter A "screening" method used to control access to your server. A filter is made up of an IP address and a subnet mask, and sometimes a port number and access type. The IP address and the subnet mask together determine the range of IP addresses to which the filter applies.

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

FTP (File Transfer Protocol) A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group directory A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among them.

guest computer An unknown computer that is not included in a computer list on your server.

guest user A user who can log in to your server without a user name or password.

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.

IANA (Internet Assigned Numbers Authority) An organization responsible for allocating IP addresses, assigning protocol parameters, and managing domain names.

ICMP (Internet Control Message Protocol) A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

idle user A user who is connected to the server but hasn't used the server volume for a period of time.

IGMP (Internet Group Management Protocol) An Internet protocol used by hosts and routers to send packets to lists of hosts that want to participate, in a process known as *multicasting*. QuickTime Streaming Server (QTSS) uses multicast addressing, as does Service Location Protocol (SLP).

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

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.

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

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

lease period A limited period of time during which IP addresses are assigned. By using short leases, DHCP can reassign IP addresses on networks that have more computers than available IP addresses.

load balancing The process of distributing the demands by client computers for network services across multiple servers in order to optimize performance by fully utilizing the capacity of all available servers.

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

local home directory A home directory that resides on disk on the computer a user is logged in to. It is accessible only by logging directly in to the computer where it resides unless you log in to the computer using SSH.

long name See *user name*.

LPR (Line Printer Remote) A standard protocol for printing over TCP/IP.

mail host The computer that provides your mail service.

managed client A user, group, or computer whose access privileges and/or preferences are under administrative control.

managed preferences System or application preferences that are under administrative control. Workgroup Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients. Macintosh Manager allows administrators to control both system preferences and application preferences for Mac OS 9 and Mac OS 8 managed clients.

MBONE (multicast backbone) A virtual network that supports IP multicasting. An MBONE network uses the same physical media as the Internet, but is designed to repackage multicast data packets so they appear to be unicast data packets.

MIBS (management information bases) Virtual databases that allow various devices to be monitored using SNMP applications.

MIME (Multipurpose Internet Mail Extension) An Internet standard for specifying what happens when a web browser requests a file with certain characteristics. A file's suffix describes the type of file it is. You determine how you want the server to respond when it receives files with certain suffixes. Each suffix and its associated response make up a MIME type mapping.

MTA (mail transfer agent) A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

multihoming The ability to support multiple network connections. When more than one connection is available, Mac OS X selects the best connection according to the order specified in Network preferences.

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

name server See *DNS (Domain Name System).*

NetBIOS (Network Basic Input/Output System) A program that allows applications on different computers to communicate within a local area network.

NetBoot server A Mac OS X server on which you have installed NetBoot software and have configured to allow clients to start up from disk images on the server.

NetInfo One of the Apple protocols for accessing a *directory domain.*

Network File System (NFS) A client/server protocol that uses TCP/IP to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

network installation The process of installing systems and software on Mac OS X client computers over the network. Software installation can occur with an administrator attending the installations or completely unattended.

nfsd daemon An *NFS* server process that runs continuously behind the scenes and processes reading and writing requests from clients. The more daemons that are available, the more concurrent clients can be served.

NSL (Network Service Locator) The Apple technology that simplifies the search for TCP/IP-based network resources.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use *LDAP, NetInfo,* or *Active Directory* protocols; *BSD* configuration files; and network services.

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

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

owner The person who created a file or folder and who therefore has the ability to assign access privileges for other users. The owner of an item automatically has read/ write privileges for that item. An owner can also transfer ownership of an item to another user.

parent A computer whose shared directory domain provides configuration information to another computer.

PHP (PHP: Hypertext Preprocessor) A scripting language embedded in HTML that is used to create dynamic webpages.

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

predefined accounts User accounts that are created automatically when you install Mac OS X. Some group accounts are also predefined.

preferences cache A storage place for computer preferences and preferences for groups associated with that computer. Cached preferences help you manage local user accounts on portable computers.

presets Initial default attributes you specify for new accounts you create using 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.

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

proxy server A server that sits between a client application, such as a web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

QTSS (QuickTime Streaming Server) A technology that lets you deliver media over the Internet in real time.

realm See *WebDAV realm.*

relay point See *open relay.*

Rendezvous A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. 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.

RTP (Real-Time Transport Protocol) An end-to-end network-transport protocol suitable for applications transmitting real-time data (such as audio, video, or simulation data) over multicast or unicast network services.

RTSP (Real Time Streaming Protocol) An application-level protocol for controlling the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. Sources of data can include both live data feeds and stored clips.

scope A group of services. A scope can be a logical grouping of computers, such as all computers used by the production department, or a physical grouping, such as all computers located on the first floor. You can define a scope as part or all of your network.

SDP (Session Description Protocol) A text file used with QuickTime Streaming Server that provides information about the format, timing, and authorship of a live streaming broadcast and gives the user's computer instructions for tuning in.

search path See *search policy.*

search policy A list of directory domains searched by a Mac OS X computer when it needs configuration information; also the order in which domains are searched. Sometimes called a search path.

shadow image A file, hidden from regular system and application software, used by NetBoot to write system-related information while a client computer is running off a server-based system disk image.

share point A folder, hard disk (or hard disk partition), or CD that is accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using *AFP,* Windows *SMB, NFS* (an "export"), or *FTP* protocols.

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

Simplified Finder A user environment featuring panels and large icons that provide novice users with an easy-to-navigate interface. Mounted volumes or media to which users are allowed access appear on panels instead of on the standard desktop.

SLP (Service Location Protocol) DA (Directory Agent) A protocol that registers services available on a network and gives users easy access to them. When a service is added to the network, the service uses SLP to register itself on the network. SLP/DA uses a centralized repository for registered network services.

SMB (Server Message Block) A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB to provide access to servers, printers, and other network resources.

SMTP (Simple Mail Transfer Protocol) A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SNMP (Simple Network Management Protocol) A set of standard protocols used to manage and monitor multiplatform computer network devices.

spam Unsolicited email; junk mail.

SSL (Secure Sockets Layer) An Internet protocol that allows you to send encrypted, authenticated information across the Internet.

static IP address An IP address that is assigned to a computer or device once and is never changed.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration.

System-less clients Computers that do not have operating systems installed on their local hard disks. System-less computers can start up from a disk image on a NetBoot server.

TCP (Transmission Control Protocol) A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

Tomcat The official reference implementation for Java Servlet 2.2 and JavaServer Pages 1.1, two complementary technologies developed under the Java Community Process.

TTL (time-to-live) The specified length of time that DNS information is stored in a cache. When a domain name–IP address pair has been cached longer than the TTL value, the entry is deleted from the name server's cache (but not from the primary DNS server).

UDP (User Datagram Protocol) A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

Unicode A standard that assigns a unique number to every character, regardless of language or the operating system used to display the language.

URL (Uniform Resource Locator) The address of a computer, file, or resource that can be accessed on a local network or the Internet. The URL is made up of the name of the protocol needed to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

USB (Universal Serial Bus) A standard for communicating between a computer and external peripherals using an inexpensive direct-connect cable.

user ID A number that uniquely identifies a user. Mac OS X computers use the user ID to keep track of a user's directory and file ownership.

user name The long name for a user, sometimes referred to as the user's "real" name. See also *short name*.

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.

WebDAV realm A region of a website, usually a folder or directory, that is defined to provide access for WebDAV users and groups.

wildcard A range of possible values for any segment of an IP address.

WINS (Windows Internet Naming Service) A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

Index