Mac OS X Server
User Management
For Version 10.6 Snow Leopard

Apple

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

019-1415/2009-05-29

Contents

About This Guide

This guide explains how to use Workgroup Manager and the command line to set up and manage accounts and preferences for clients.

Mac OS X Server includes Workgroup Manager, a user management tool you can use to create and manage accounts. Mac OS X Server also allows you to use the command line to create and manage accounts.

When managing accounts, you can define core account settings like name, password, home folder location, and group membership. You can also manage preferences, allowing you to customize the user's experience, granting or restricting access to his or her computer's settings and to network resources.

Workgroup Manager works closely with a directory domain. Directory domains are like databases but are specifically designed for storing account information and handling authentication.

What's New in Workgroup Manager

- **Improved augmented record support.** Augmented user records are imported user accounts that allow you to enable specific settings such as the user's login picture, or to manage preferences.

  These settings are specific to the augmented record. You don't need to edit the accounts stored in the original directory domain. The settings you aren't allowed to edit are synced with the directory domain they're imported from.

  You can use augmented user records to manage preferences for accounts stored in an Active Directory domain or in an Open Directory domain that you don't have editing permissions for. For more information, see "Creating Augmented User Records" on page 57.

- **External accounts support MS-DOS (FAT) format.** External accounts are supported on external drives that use the MS-DOS (FAT) format.

An external account is a mobile account that has its local home folder stored in a volume on an external drive. The portable home directory is created from the local home folder stored on that external drive and the user's network home folder.

External accounts now support external or ejectable volumes formatted as Mac OS X Extended format (HFS Plus) or MS-DOS format (FAT). For more information, see "About External Accounts" on page 145.

What's in This Guide

This guide includes the following sections:

- Chapter 1, "User Management Overview," highlights important concepts, introduces user management tools, and tells you where to find additional information about user management and related topics.
- Chapter 2, "Getting Started with User Management," provides planning and setup information to create a user management environment.
- Chapter 3, "Getting Started with Workgroup Manager" describes how to set up Workgroup Manager and use its core features.
- Chapters 4, 5, and 6 explain how to use Workgroup Manager to set up users, groups, computers, and computer groups.
- Chapter 7, "Setting Up Home Folders," covers creating home folders.
- Chapter 8, "Managing Portable Computers," details considerations for managing portable computers.
- Chapter 9, "Client Management Overview," introduces client management tools and concepts, such as how to customize a user's work environment and provide user access to network resources.
- Chapter 10, "Managing Preferences," describes how to use Workgroup Manager to control preference settings for users, groups, computers, and computer groups that use Mac OS X.
- Chapter 11, "Solving Problems," helps you address issues involving account creation, home folder maintenance, preference management, and client setup, and also helps you solve problems encountered by managed clients.

The appendix, "Importing and Exporting Account Information," provides information you need to transfer account information to or from an external file.

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

Using Onscreen Help

You can get task instructions onscreen in the Help Viewer application while you're managing Mac OS X Server v10.6. You can view help on a server or an administrator computer. (An administrator computer is a Mac OS X computer with Mac OS X Server administration v10.6 software installed on it.)

To get the most recent onscreen help for Mac OS X Server v10.6:

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

To see the most recent server help topics:

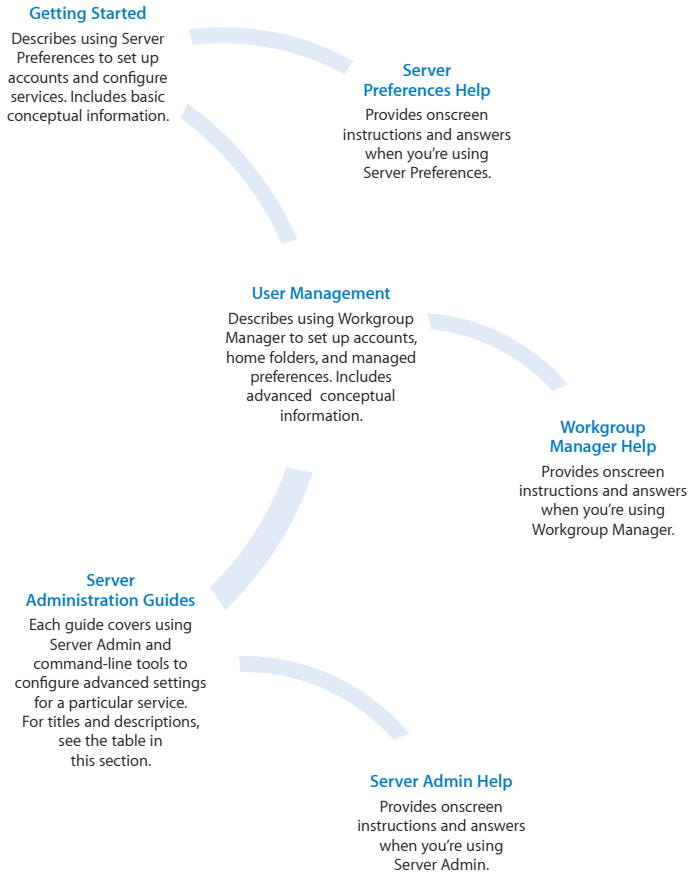
- Make sure the server or administrator computer is connected to the Internet while you're getting help.

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

Documentation Map

Mac OS X Server v10.6 has a suite of guides which can cover management of individual services. Each service may be dependent on other services for maximum utility. The documentation map below shows some related documentation that you may need to fully configure your desired service to your specifications. You can get some of these guides in PDF format from the Mac OS X Server documentation website:

www.apple.com/server/resources/



Viewing PDF Guides Onscreen

While reading the PDF version of a guide onscreen:

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

Printing PDF Guides

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

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

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

Getting Documentation Updates

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

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

  www.apple.com/server/resources/
- An RSS feed listing the latest updates to Mac OS X Server documentation and onscreen help is available. To view the feed use an RSS reader application, such as Safari or Mail:

  feed://helposx.apple.com/rss/snowleopard/serverdocupdates.xml

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—get important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx/)—enter the gateway to extensive product and technology information.

- *Mac OS X Server Support website* (www.apple.com/support/macosxserver/)—access hundreds of articles from Apple's support organization.
- *Apple Discussions website* (discussions.apple.com/)—share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com/)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Training and Certification website* (www.apple.com/training/)—hone your server administration skills with instructor-led or self-paced training, and differentiate yourself with certification.

User Management Overview

1

Use this chapter to learn user management concepts and the applications used to manage accounts and privileges.

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

Tools for User Management

User management tools and technologies in Mac OS X Server include Workgroup Manager, Server Admin, Server Preferences, and command-line tools.

Workgroup Manager

Workgroup Manager is a powerful tool that delivers features for comprehensive management of Macintosh clients.

You can use Workgroup Manager on a computer with Mac OS X or Mac OS X Server installed. Workgroup Manager included with Mac OS X Server v10.6 can manage client computers running Mac OS X v10.4 or later.

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

You use Workgroup Manager to create user accounts and set up groups to provide convenient access to resources. You can:

- Use account settings and managed preferences to achieve the level of administrative control you need, while making the user experience more efficient
- Manage Finder, login, media access, and print settings
- Control access to computers and restrict the applications allowed to run on them

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

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

To get started with Workgroup Manager, see Chapter 3, "Getting Started with Workgroup Manager."

Server Admin

The Server Admin application provides access to various tools and services that play a role in server management.

After installing the Mac OS X Server software, use Server Admin to set up directory services and establish your network. Then use Workgroup Manager to create and manage accounts. After that, use Server Admin to set up additional services to provide mail service, host websites, share printers, and create share points (which allow users to share folders and files).

For information about how to use the many services managed through Server Admin, see the service administration guides. The following table lists common server administration tasks and includes the location of related documentation.

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

Server Preferences

You can use Server Preferences to configure key features of collaboration and file services. Its streamlined approach allows novice system administrators to quickly configure a server without requiring much technical knowledge.

You can also use Server Preferences to configure user and group accounts (such as setting passwords, enabling services, and assigning group membership), but not computer or computer group accounts. However, you can't use Server Preferences to manage user preferences.

For more information, see *Getting Started* and *Server Preferences Help*.

Command-Line Tools

Mac OS X Server v10.6 includes several client-management command-line tools. For example, the `dscl` tool allows you to view and edit account settings and manage preferences, while the `mcxquery` tool reports the managed preferences that are effective for a particular user.

Use the `mcxquery` tool to review how combined and overridden managed preferences interact at the user, group, computer, or computer group level. The tool also determines which directory domain stores those managed preference settings.

This guide describes how to perform many tasks from Workgroup Manager and the command line.

Accounts

To manage accounts, you use an administrator account. With an administrator account, you can set up and manage the following account types:

- User accounts
- Group accounts
- Computer accounts
- Computer groups

When creating a user account, you must specify a user name and password, which are needed to prove the user's identity. You can also specify a user identification number (user ID or UID), which is used for folder and file permissions.

Other user account information is used by various services to determine what the user is authorized to do and to personalize the user's environment.

In addition to the accounts you create, Mac OS X Server also has predefined user and group accounts, some of which are reserved for use by Mac OS X.

Administrator Accounts

Users with server administration or directory domain administration privileges are known as *administrators.* An administrator can be a server administrator, directory administrator, or both.

Server administrator privileges determine whether a user can change the settings of a server.

Directory administrator privileges determine the extent to which an administrator can change account settings for users, groups, computers, and computer groups in the directory domain.

Server Administration

Server administration privileges determine the functions available to a user when logged in to a Mac OS X Server. For example, a server administrator can use Directory Utility to make changes to a server's search policy.

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

Local Mac OS X Computer Administration

Any user who belongs to the admin group in the local directory domain has administrator privileges on that computer. If you add a group from another directory domain to the admin group of the local directory domain, members of that group become administrators on the computer.

Limited Administration

You can control the extent to which a limited administrator can use Workgroup Manager to change account data stored in a domain.

For example, you can set up directory domain privileges so your network administrator can add and remove user accounts but allow limited administrators to change the information for users, or you can designate multiple limited administrators to manage different groups.

For more information, see "Giving a User Limited Administrative Capabilities" on page 73.

Directory Domain Administration

When you create a directory domain in Mac OS X Server, a directory administrator account is created and added to the admin group in the domain.

If you plan on connecting your directory domain to other directory domains, choose a unique user name and ID for each directory administrator.

When you assign full directory domain administration privileges to a user, the user is added to the "admin" group in the directory domain. This does not grant the user local admin privileges on the servers hosting this directory domain or on any other servers or clients bound to this directory domain.

Each directory domain has a directory administrator account, and a directory administrator can create additional directory administrators in the same domain. Any user with a user account in a directory domain can be made a directory administrator (an administrator of that domain).

For more information, see "Giving a User Full Administrative Capabilities" on page 75.

User Accounts

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

Most users have an individual account used to authenticate them and control their access to services. When you want to personalize a user's environment, you define user, group, computer, or computer group preferences for that user.

The term *managed client* or *managed user* refers to a user who has administrator-controlled preferences associated with his or her account. *Managed client* is also used to refer to computers or computer groups that have preferences defined for them.

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

Guest Account

You can provide services for users who can't be authenticated because they don't have a valid user name or password. These users are known as *guest users*. If your computers run Mac OS X v10.5 or later, you can enable a guest account, which is specifically designed for guest users.

The guest account allows anonymous access to a computer. The guest account has a local home folder that has its contents erased when the user logs in or out of the guest account.

The guest account is best used for common-access computers, such as those in a library or open lab where you might not need to log user access and where the user maintains his or her files separate from the local computer.

For some services, like Apple Filing Protocol (AFP), you can let guest users access files. Instead of authenticating with a name and a password, a guest user connects as a guest, not as a registered user. Guests are restricted to files and folders with permissions set to Everyone.

Group Accounts

To ease user administration, you can create group accounts. A group is a collection of users or other groups who have similar needs. For example, you can add all English teachers to one group and allow that group to access specific files or folders on a volume.

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

Use group account settings to control user access to folders and files. For more information, see "Folder and File Access by Other Users" on page 27.

A group can be a member of another group. A group that contains another group is called a *parent group*. The group contained in the parent group is called a *child hierarchical group* or just *hierarchical group*. Hierarchical groups are useful for inheriting access permissions and managed preferences.

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

Workgroups

When you define preferences for a group, it becomes a *workgroup*. A workgroup lets you manage the work environment of group members.

Workgroup preferences are stored in the group account. For a description of workgroup preferences, see Chapter 10, "Managing Preferences."

Group Folders

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

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

Computer Accounts

Computer accounts allow you to identify and manage individual computers.

To create a computer account, you need the computer's Ethernet ID. When creating the account, you can also associate it with an IP address. After creating the account, you can manage its preferences or add it to a computer group.

For more information about setting up computer accounts, see Chapter 6, "Setting Up Computers and Computer Groups." To specify preferences for Mac OS X computer accounts, see Chapter 10, "Managing Preferences."

Guest Computers

Most computers on your network should have a computer account. If an unknown computer (one that doesn't have a computer account) connects to your network and attempts to access services, that computer is treated as a *guest*. Settings chosen for the Guest Computer account apply to unknown guest computers.

Computer Groups

A computer group is composed of computer accounts or computer groups. By combining these into a single computer group, you can apply the same managed preferences to all its members.

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

The User Experience

After you create an account for a user, the user can access server resources according to the permissions you set.

The user experience depends on the type of user, permissions set, type of client computer in use (such as Windows or UNIX), whether the user is a member of a group, and whether preference management is implemented at the user, group, or computer level.

For more information about the Mac OS X user experience, see Chapter 9, "Client Management Overview." Basic information about authentication, identity validation, and information-access control is given in the following sections.

Authentication and Identity Validation

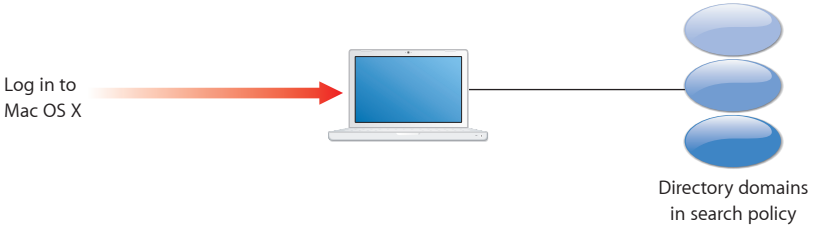
Before a user can log in or connect to a Mac OS X computer, he or she must enter a name and password associated with a user account accessible by the computer.

A Mac OS X computer can access user accounts that are stored in a directory domain. To access accounts stored in the directory domain, the directory domain must be listed in the search policy of your computer.

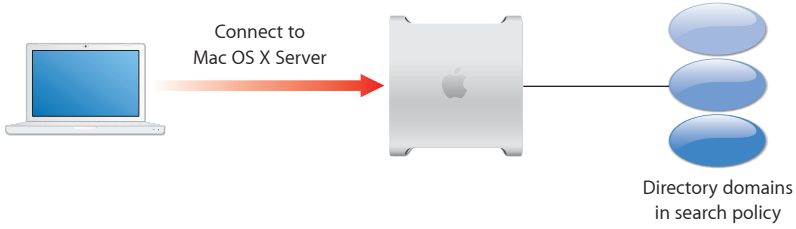
A *directory domain* stores information about users and resources. The domain maintains a database the computer accesses to retrieve configuration information.

A *search policy* is a list of directory domains that the computer searches when it needs configuration information, starting with the local directory domain on the user's computer.

The following illustration shows a user logging in to an account in a directory domain in the computer's search policy.



After login, the user can connect to a remote server to access its services (if the user's account is located in the server's search policy).



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

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

For more information about types of directory domains and instructions for configuring search policies, see *Open Directory Administration*. It also discusses authentication methods and provides instructions for setting up user authentication options.

Information Access Control

To control access to information, a universal ID called a *globally unique identifier* (GUID) provides user and group identity for access control list (ACL) permissions.

An ACL is a list of access control entries (ACEs), each specifying the permissions to be granted or denied to a group or user, and how these permissions are propagated throughout a folder hierarchy. The GUID also associates a user with group and hierarchical group memberships.

Prior to Mac OS X v10.4, Mac OS X used user ID and POSIX permissions to track folder and file permissions. In Mac OS X, folders or files include POSIX permissions for entities such as:

- Owner
- Group
- Everyone else

Because GUIDs are 128-bit values, duplicate GUIDs are extremely unlikely. For example, compare the following example values:

Identification type	Example value
short name	ajohnson
user ID	1005
GUID	C7B063D4-0260-44D6-829B-DCD5A99DB3EC

Unlike ACL permissions, POSIX permissions can cause file-ownership and group-membership issues when multiple users have identical short names or user IDs. When using GUIDs, users with the same short name or user ID can have different ACL permissions.

The introduction of GUIDs does not change or remove POSIX permissions, so it does not affect the interoperability of Mac OS X with legacy UNIX systems or other operating systems.

Folder and File Owner Access

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

If you change a user ID, the user might not be able to modify or access files and folders he or she created. Likewise, if the user logs in as a user whose user ID is different from the user ID he or she used to create the files and folders, the user no longer has owner permissions for those files and folders.

Folder and File Access by Other Users

The use of GUIDs in conjuction with ACLs determines the files that users and groups can access. Also, the user ID, in conjunction with a group ID, is used to control access.

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

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

ACLs and POSIX Permissions

Every file and folder has POSIX permissions. Unless an administrator assigns ACL permissions, POSIX permissions continue to define user access. If you assign ACL permissions, they take precedence over standard POSIX permissions.

If a file has ACL permissions but none apply to the user, the POSIX permissions determine user access. If a file has multiple ACEs that apply to a user, the first applicable ACE takes precedence, and subsequent ACEs are ignored.

For more information about ACL and POSIX permissions, see *File Server Administration*.

SIDs and Windows Interoperability

Mac OS X computers work seamlessly with Windows computers because Mac OS X assigns a security identifier (SID) to a process or file when it assigns a GUID to the process or file. An SID is a Windows identifier that has similar functionality to a GUID on a Mac OS X computer.

When Windows users access share points using Server Message Block (SMB), they transfer SIDs, not GUIDs. When Mac OS X Server receives SIDs, it retrieves the user accounts with the corresponding GUIDs.

Windows servers use Active Directory as their directory domain. If a user account is moved to a different Active Directory domain, it receives a new SID but not a new GUID. The user still has access permissions assigned to old SIDs because Active Directory keeps track of SID history in user accounts.

Getting Started with User Management

2

Use this chapter to learn how to plan and set up a user management environment.

To create an effective user management environment, you must carefully plan your network. Then, when deploying the network, you must systematically and methodically set up your network resources.

Setup Overview

This section provides an overview of user management setup tasks, including the sequence of stages an administrator follows to create a managed environment. Not all steps are necessary in every case.

For a more comprehensive approach to planning, security, server setup, installation and deployment, management, and monitoring, see *Server Administration*.

Step 1: Before you begin, do some planning Analyze your users' needs to determine which directory service configuration and home folder setup is the most suitable. For more information, see "Planning Strategies for User Management" on page 32.

Step 2: Set up the server infrastructure Before deploying client computers, make sure a computer with Mac OS X Server is set up for hosting accounts and share points. New servers come with Mac OS X Server software preinstalled.

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

There are different kinds of shared directories. You can use Workgroup Manager to add or modify accounts that reside in read/write directory domains such as an Open Directory domain or the local directory domain.

Make sure read-only directory domains (such as LDAPv2, read-only LDAPv3, or BSD flat files) are configured to support Mac OS X Server and that they provide necessary account data.

To make the directory compatible, you might need to add, modify, and reorganize directory information.

Mac OS X offers various options for authenticating users (including Windows users) whose accounts are stored in directory domains on Mac OS X Server. In addition, Mac OS X accesses accounts in existing directories on your network, such as an Active Directory hosted on a Windows server.

To make network home folders, group folders, and other shared folders available on the network so users can access them from different computers, use file services.

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

The following administration guides describe infrastructure setup in detail:

- For installation requirements and guidelines, see *Getting Started*.
- For information about installation and setup of server software, see *Server Administration*.
- For information about directory services and authentication, see *Open Directory Administration*.
- For information about how to set up file services, see *File Server Administration*.

Step 3: Set up an administrator computer Because servers are usually kept in a secure, locked location, administrators typically conduct user management tasks remotely from a Mac OS X computer. Such a computer is referred to as an *administrator computer*.

Before you can use an administrator computer to create and manage accounts in a shared directory, you must have a user account in the shared directory and you must be a directory administrator. A directory administrator can use Workgroup Manager to add and change accounts in an Open Directory domain or another read/write directory domain.

To set up an administrator computer and create directory administrator accounts, see Chapter 3, "Getting Started with Workgroup Manager."

Step 4: Set up a home folder share point Home folders for accounts stored in shared directories can reside in a network share point accessible by the user's computer.

You can set up network home folders so they can be accessed using AFP or NFS, or you can set up home folders for exclusive use by Windows users using SMB.

For information about setting up home folders using AFP, NFS, or SMB, see Chapter 7, "Setting Up Home Folders."

Step 5: Create user accounts and home folders You can use Workgroup Manager to create user accounts in directories that reside on Mac OS X Server or in other read/write directory domains. The following sections contain instructions for creating accounts and folders:

- To create user accounts, see Chapter 4, "Setting Up User Accounts."
- To create mobile user accounts, see Chapter 8, "Managing Portable Computers."
- To set up home folders, see Chapter 8, "Managing Portable Computers."

Step 6: Set up client computers Mac OS X Server supports users of Mac OS X, Windows, and UNIX client computers.

For Mac OS X computers, configure the search policy of the computers so it locates shared directory domains. For instructions, see *Open Directory Administration*.

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

You can join Windows workstations to the Mac OS X Server primary domain controller (PDC), which is similar to the way you configure Windows workstations to join a Windows NT server domain.

If you have more than a few Macintosh client computers to set up, consider using NetInstall to create a system image that automates client computer setup. For instructions, see *System Imaging and Software Update Administration*.

To prevent unauthorized access to client computers, secure them from local and network threats. For information, see *Mac OS X Security Configuration*.

Step 7: Define user account preferences You manage the work environment of Macintosh users whose accounts reside in a shared domain by defining user account preferences. For information about Mac OS X user preferences, see Chapter 9, "Client Management Overview" and Chapter 10, "Managing Preferences."

Step 8: Create group accounts and group folders Use Workgroup Manager to create group accounts in directories that reside on Mac OS X Server and in other read/write directory domains.

You can create group folders to distribute documents and organize group member applications. You can also set up ACLs and other access privileges to restrict a group's access to folders or files:

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

Step 9: Define group account preferences You can manage preferences for a group account. A group account with managed preferences is called a *workgroup*. For information about Mac OS X workgroups, see Chapter 9, "Client Management Overview" and Chapter 10, "Managing Preferences."

Step 10: Define computer accounts, computer groups, and preferences Use computer accounts or computer groups to manage Macintosh client computers.

- For information about creating Mac OS X computer accounts or computer groups, see Chapter 6, "Setting Up Computers and Computer Groups."
- For information about computer group preferences, see Chapter 9, "Client Management Overview" and Chapter 10, "Managing Preferences."

Step 11: Perform ongoing account maintenance As users come and go and the requirements for your servers change, you must update account information:

- For information about how to use Workgroup Manager to display accounts, see Chapter 3, "Getting Started with Workgroup Manager."
- For information about how to perform common tasks such as creating accounts, disabling accounts, adding and removing users from groups, and deleting accounts, see Chapter 4, "Setting Up User Accounts" through Chapter 6, "Setting Up Computers and Computer Groups."
- For solutions to common problems, see Chapter 11, "Solving Problems."

Planning Strategies for User Management

The following are planning activities to undertake before you implement user management.

Analyzing Your Environment

Your environment defines your user management settings, including:

- Size and distribution of your network
- Number of users who access your network
- Type of computers used (Mac OS X or Windows)
- How client computers are used
- Which computers are mobile
- How to define security and password policies
- Which users should have administrator privileges
- Which users should have access to specific computers
- What services and resources users need (such as mail or access to data storage)
- How to divide users into groups (for example, by class topic or job function)
- How to group computers (such as all computers in a public lab)

Identifying Directory Services Requirements

Identify the directories where you'll store user and group accounts, computers, and computer groups:

- Set up an Open Directory master and replicas to host a Lightweight Directory Access Protocol (LDAP) directory for storing other user accounts, group accounts, computers, and computer groups on your network. For information about password handling options, see *Open Directory Administration*.
- If you have an earlier version of an Apple server, you might be able to migrate existing records. For available options, see *Updating and Migrating*.
- If you have an LDAP or Active Directory server set up, you might be able to use existing account records. For details about accessing existing directories, see *Open Directory Administration*.

  For information about working with Open Directory groups and computer groups, see Chapter 5, "Setting Up Group Accounts" and Chapter 6, "Setting Up Computers and Computer Groups."

Note: If all domains are not finalized when you're ready to start adding user and group accounts, add the accounts to any directory domain that exists on your server. (The local directory domain is always available.) You can move users and groups to another directory domain later by using your server's export and import functions.

Passwords are not retained when exporting and importing account information. However, they are retained if you archive and restore the directory domain. For more information, see the appendix, "Importing and Exporting Account Information."

Determining Server and Storage Requirements

When planning for server needs, you must first acquire the following information:

- The number of concurrently connected computers, which affects network traffic and server response times
- The number of user accounts, which affects the amount of storage space required to store user files

Directory services, including authentication and user management, require one Open Directory master or replica for every 1000 computers, regardless of the number of total user accounts.

For example, if you have 400 computers and 2000 users, you need one Open Directory master for authentication and account management. If you have 1800 computers and 2500 users, you need one Open Directory master and one Open Directory replica.

If you use network home folders, they require one dedicated home folder server for every 150 concurrent connections. If you use mobile accounts with portable home directories, you need one dedicated home folder server for every 300 concurrent connections.

For example, if you have 400 computers and 2000 users on network home folders, you need three dedicated home folders servers. If those users are deployed with portable home folders, you need two dedicated home folder servers.

If you have 1800 computers and 2500 users, you should have 12 dedicated home folder servers for network home folders and 6 dedicated servers for portable home directories.

Group folders require one server for every 450 concurrent connections. For example, if you have 400 computers, you need one group folder server. For 1800 computers, you need four group folder servers.

Storage requirements vary because users have varying storage needs. Some users might store very few files in their home folders, while other users fill theirs. A simple guideline is to start with 1 gigabyte (GB) of storage per user account, but allow for expansion.

Don't establish disk quotas or other space restrictions unless you have closely examined your users' storage needs. For example, 2000 user accounts might only need 2 terabytes (TB) of storage over the course of several years. However, if you give that same 2000 users their own computers with 60 GB drives, they could use as much as 120 TB of storage. In this case, every user fills his or her drive and then portable home directory syncing mirrors files from his or her local home folder to the network file server.

The following table summarizes the above requirements:

Requirement	Maximum value
Computers connected to each directory server	1000
Network home folders per file server	150
Portable home folders per file server	300
Group folder concurrent connections per server	450

Choosing a Home Folder Structure

When deploying computers, one of the most crucial decisions is choosing how and where to host home folders.

There are three types of home folders: a local home folder, a network home folder, and a portable home directory. These home folders are typically tied, respectively, to local, network, and mobile accounts.

When considering your home folder structure, keep the following in mind:

- **Users with local accounts typically have local home folders.**

  When users save files in local home folders, the files are stored locally. To save the files over the network, users must connect to the network and upload the files.

  Using local home folders provides the least amount of control over a user's managed preferences and is also not inherently tied to a network account.

- **Users with network accounts typically have network home folders.**

  When users save files in network home folders, the files are stored on the server. When users access home folders, even for common tasks like caching webpages, the files are retrieved from the server.

  Using network home folders provides complete control over a user's managed preferences. When users are not connected to the network, they can't access their accounts or home folders.

- **Users with mobile accounts have local and network home folders, which combine to form portable home directories.**

  When users save files, the files are stored in a local home folder. The portable home directory is a synced subset of a user's local and network home folders. You can configure which folders to sync and how frequently to sync them.

  Mobile accounts also cache authentication information and managed preferences. If you sync key folders, a user can work on and off the network and experience a seamless work environment.

  If you choose not to sync portable home directories, mobile accounts are then very similar to local accounts, except that mobile accounts have managed preferences.

- **Users with mobile accounts who access their accounts on computers running Mac OS X v10.5 or later can use portable home directories with an external drive.**

  When users connect external drives to a computer (including computers off of the network), they can still access their accounts. These types of mobile accounts are called *external accounts.*

  An external account stores its local home folder on the external drive and doesn't create a local home folder on the computer it's accessed from.

  Except for the location of the local home folder, external accounts are treated like mobile accounts, with the same kinds of syncing, cached authentication, and managed preference benefits.

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

Mobile accounts and external accounts are described in detail in Chapter 8, "Managing Portable Computers."

Devising a Home Folder Distribution Strategy

Determine which users need home folders and identify the computers where you want these home folders to reside. For performance reasons, avoid using network home folders over network connections slower than 100 megabits per second (Mbit/s).

A user's network home folder doesn't need to be stored on the same server as the directory containing the user's account. In fact, distributing directory domains and home folders across multiple servers can help balance your network load. This scenario is described in "Distributing Home Folders Across Multiple Servers" on page 125.

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

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

When determining the access protocol to use for home folders, AFP is most commonly used in a Mac-based computer environment. If you are hosting home folders on UNIX servers that do not support AFP, you might want to use NFS. If you are hosting home folders on Windows servers, you might want to use SMB.

For more information about how to use these protocols for home folders, see "About Home Folders" on page 123.

Identifying Groups

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

Determining Administrator Requirements

You don't need to give full directory administrator privileges to all users who need only *some* administrative control. Instead, you can give them limited administrative privileges.

Decide which users will have full administrative control over accounts and which users will perform only a few administrative duties.

The directory administrator has the greatest amount of control over other user accounts and privileges. The directory administrator can create user accounts, group accounts, computer accounts, and computer groups, and can assign settings, privileges, and managed preferences for them. He or she can also create other server administrator accounts, or give specific users (for example, teachers or technical staff) administrator privileges in specified directory domains.

Limited administrators can perform common administrative tasks for specified users and groups. They can manage user preferences, edit managed preferences, edit user information, and edit group membership. Giving users limited administrative privileges helps them to be more self-sufficient, without putting your organization at risk.

For example, you might want to give student lab assistants the ability to manage user passwords for a small group of students, while giving teachers the ability to manage user passwords, edit user information, and edit group information for all of their classes.

Because users can be given limited administrator privileges, consider which users require directory administrator privileges. A well-planned hierarchy of administrators and users with special administrator privileges helps you distribute system administration tasks and makes workflow and network management more efficient.

When you use Server Assistant to configure your server, specify a password for the owner/administrator. This password also becomes the root password for your server.

Changing the owner/administrator password doesn't affect the root password. Only a few server administrators need to know the root password, because you can usually use the `sudo` command to use command-line tools (such as `CreateGroupFolder`).

Administrators who don't need root access can use Workgroup Manager to create an administrator user with a password different from the root password.

Use the root password with caution and store it in a secure location. The root user has full access to the system, including system files. If necessary, you can use Workgroup Manager to change the root password.

Getting Started with Workgroup Manager

3

Use this chapter to set up Workgroup Manager and use its core features.

Workgroup Manager is the primary application for managing client computers. You can use Workgroup Manager to create accounts and manage preferences.

Configuring the Administrator's Computer and Account

To use Workgroup Manager, you must first install the Mac OS X Server administration tools. Before you can manage client computers, you must configure a computer for use as an administrator computer and create a directory administrator account.

Setting Up an Administrator Computer

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

The computer should have Mac OS X v10.5 or later, at least 512 MB of RAM, and 1 GB of unused disk space.

For more about server and storage requirements, see "Determining Server and Storage Requirements" on page 33.

To create and modify accounts, you must also have a directory administrator account.

To set up an administrator computer:

1 Insert the *Administration Tools* disc and then start the installer, ServerAdministrationSoftware.mpkg, located in the /Installers folder.

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

You can also download the latest Administration Tools disc image from the *Mac OS X Server Support website* (www.apple.com/support/macosxserver/).

2. Follow the onscreen instructions.
3. After installing the administration tools, run Software Update (choose Apple > Software Update) to ensure you have the latest version of the tools.
4. If you are managing preferences that use specific paths to find files (such as Dock preferences), make sure the administrator computer has the same file system structure as each managed client computer.

   This means that folder names, volumes, the location of applications, and so on should be the same.
5. Add the directory domain to the directory services of the administrator computer.

   In System Preferences, click Accounts, select Login Options, and then click Join.

   To add a directory domain to the search policy for *both* authentication and contacts, enter your directory domain's information, click OK, and authenticate as a local administrator if requested.

   To add a directory domain to the search policy for *either* authentication or contacts, click Open Directory Utility. For information on using Directory Utility, view Directory Utility Help.

Creating a Directory Administrator Account

Before creating and editing accounts in a shared directory, you need a directory administrator account in the directory. A directory administrator can use Workgroup Manager to add and change accounts residing in an Open Directory domain, the local directory domain, or another read/write directory domain.

To create a directory administrator account:

1. On the administrator computer, open Workgroup Manager and authenticate as the administrator user created during server setup.
2. Access the shared directory by clicking the globe icon and choosing the directory domain.

   If you're not authenticated, click the lock and enter the name and password of a directory administrator.
3. Click New User, click Basic, and then provide basic information for the administrator.
4. Click Privileges and from the "Administration capabilities" pop-up menu choose Full.
5. Click Save.

From the Command Line

You can also create a directory administrator account using the `dscl` command in Terminal. For more information, see "Creating User Accounts" on page 53.

Using Workgroup Manager

After installing the Mac OS X Server software and setting up a directory administrator account, you can access and use Workgroup Manager for user management.

This section provides an introduction to Workgroup Manager.

Using Mac OS X Server v10.6 to Administer Earlier Versions of Mac OS X

Server Admin for Mac OS X v10.6 can connect to Mac OS X Server v10.5.6 or later. You can use Workgroup Manager included with Mac OS X v10.6 to manage client computers running Mac OS X v10.4 or later.

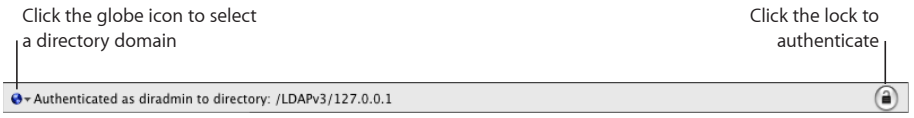
Connecting and Authenticating to Directory Domains in Workgroup Manager

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

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

To connect and authenticate to directory domains:

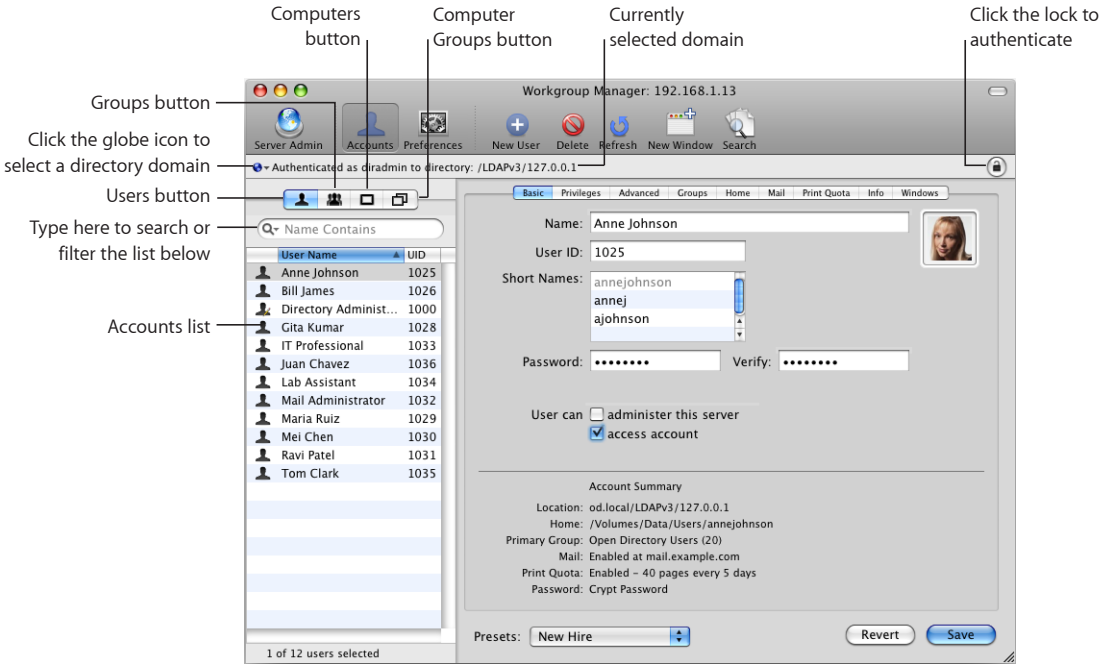
1. Open Workgroup Manager and from the Workgroup Manager Connect window click Browse, or enter the IP address or DNS name for a server that connects to directory domains.
2. Enter the user name and password for a directory administrator and click Connect.
3. To change directory domains while connected to a server, click the globe icon (see below) to select a domain, then authenticate as a directory administrator by clicking the lock icon.



4. To connect to a different server, choose Server > Connect.

Major Workgroup Manager Tasks

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



Here is how to get started with primary Workgroup Manager tasks:

- To specify the directory domain that stores accounts you want to work with, click the globe icon.
- To work with accounts in different directories at the same time or to work with different views of accounts in a directory, open multiple Workgroup Manager windows by clicking the New Window icon in the toolbar or by choosing Server > New Workgroup Manager Window.
- To administer accounts in the selected directory, click the Accounts icon in the toolbar; then click the Users, Groups, Computers, or Computer Groups button on the left side of the window to list the accounts that exist in the directories you are working with.
- To filter the displayed account list, use the pop-up search menu above the accounts list.
- To work with managed preferences, select an account (or several accounts) and then click the Preferences icon in the toolbar.
- To import or export user and group accounts, choose Server > Import or select the accounts and choose Server > Export.

- To view onscreen help, use the Help menu. The Help menu gives you access to help for administration tasks available through Workgroup Manager and other Mac OS X Server topics.
- To open Server Admin so you can monitor and work with services on a server, click the Server Admin icon in the Workgroup Manager toolbar.

  For information about Server Admin, see *Server Administration*.

Modifying Workgroup Manager Preferences

You can change Workgroup Manager preferences to customize how records are displayed and to enable the Inspector, which is an advanced directory domain editor.

Workgroup Manager includes the following preferences.

Preference	Description
Resolve DNS names when possible	(Default: on) Disabling this preference causes Workgroup Manager to stop resolving DNS names when writing data. If you're having DNS issues, disabling this can help mitigate the effect of those DNS issues (but you should fix those issues).
Show "All Records" tab and inspector	(Default: off) Enabling this preference enables the Inspector. The Inspector allows you to see and edit directory data not otherwise visible in Workgroup Manager. For more information, see Server Admin Help.
Limit search results to requested records	(Default: off) When you don't enter anything in the search field, by default, Workgroup Manager lists all user records in the selected directory domain. Disabling this preference requires you to enter "*" (without quotes) to list all records, which can expedite working with large directory domains in Workgroup Manager (because Workgroup Manager doesn't automatically list all records).
List a maximum of # records	(Default: off) Enabling this preference limits the maximum number of search results to a number you specify. Enabling this preference and setting a reasonable maximum number can improve Workgroup Manager performance. However, setting the number too low can cause you to overlook the total number of matches.

To set Workgroup Manager preferences:

1. In Workgroup Manager, choose Workgroup Manager > Preferences.
2. Select the preferences you want to change.

3 To reset the warning messages you've marked as "Don't show again," click "Reset 'Don't show again' messages."

4 Click OK.

Finding and Listing Accounts

Workgroup Manager provides several methods for finding and listing user accounts, group accounts, computer accounts, and computer groups.

Working with Account Lists in Workgroup Manager

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

The following settings influence the contents and appearance of the list:

- Workgroup Manager preferences can limit the maximum number of records shown and whether you want to enable the Inspector (which allows you to view or edit raw directory data). To set up Workgroup Manager preferences, choose Workgroup Manager > Preferences.

  Open Directory can also limit the maximum number of records shown, so even if you don't set a maximum number in Workgroup Manager, you might see a subset of the total number of records.

- The list reflects the directory you've chosen from the globe icon. If you connect to the directory server, the accounts in the parent directory domain are listed. If you do not connect to the directory server, local accounts are listed.

  The listed domains are the local directory domain, all directory domains in the server's search policy, and all available directory domains (domains the server is configured to access, even if not in the search policy). For instructions on configuring a server to access directory domains, see *Open Directory Administration*.

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

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

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

Listing Accounts in the Local Directory Domain

When you list accounts in the local directory domain, you list all local accounts. These local accounts can only be accessed by users of the local computer or server, not by users of client computers.

Services and programs running on a server can access the server's local directory domain. Programs running on a client computer, such as the client computer's login window, can't access the server's local directory domain.

If a server hosts file services, users with accounts from the server's local directory domain can authenticate with the file services.

User accounts from the server's local directory domain 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 globe icon and choose Local.

   For servers running Mac OS X Server v10.5 or later, the local directory domain is listed as /Local/Default.

2. Choose from the following:
   - To view user accounts, click the Users button.
   - To view group accounts, click the Groups button.
   - To view computer accounts, click the Computers button.
   - To view computer groups, click the Computer Groups button.
3. To work with an account, select it.

   Changing account settings or preferences requires server administrator privileges, so you might need to click the lock to authenticate.

Listing Accounts in Search Policy Directory Domains

A computer's search policy specifies which directory domains Open Directory can access. The search policy also specifies the order in which Open Directory accesses directory domains. By listing accounts in a search policy, you list the accounts on all directory domains in the search policy.

You can't edit accounts when listing accounts in a search policy.

For more information about how to set up search policies, see *Open Directory Administration*.

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

1. In Workgroup Manager, connect to a server that has a search policy containing the directory domains of interest.
2. Click the globe icon and choose Search Policy.
3. Choose from the following:
   - To view user accounts, click the Users button.
   - To view group accounts, click the Groups button.
   - To view computer accounts, click the Computers button.
   - To view computer groups, click the Computer Groups button.

Listing Accounts in Available Directory Domains

Using Workgroup Manager, you can list user accounts, group accounts, computer accounts, and computer groups residing in any available directory domain accessible from the server you're connected to.

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

To learn how to configure access to directory domains, see *Open Directory Administration*.

To list accounts in a directory domain accessible from a server:

1. In Workgroup Manager, connect to a server where you can access the directory domains.
2. Click the globe icon and then choose the domain where the user's account resides.

   If the directory domain is not listed, add it to the pop-up menu by choosing Other. In the dialog that appears, select the domain and then click OK.
3. Choose from the following:
   - To view user accounts, click the Users button.
   - To view group accounts, click the Groups button.
   - To view computer accounts, click the Computers button.
   - To view computer groups, click the Computer Groups button.
4. To work with an account, select it.

   Changing the account requires directory administrator privileges, so you might need to click the lock to authenticate.

Refreshing Account Lists

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

To refresh account lists, click Refresh in the toolbar. Alternatively, click the globe icon and then choose the directory domain you're working in from the pop-up menu.

Finding Specific Accounts in a List

After you've displayed a list of accounts in Workgroup Manager, you can filter the list to find specific users or groups.

You can choose from several filters:

- Name Contains
- Name Starts With
- Name Ends With
- Name Is
- ID Is
- ID Is Greater Than
- ID Is Less Than
- Comment Contains
- Keyword Contains

To filter items in the list of accounts:

1. After listing accounts, click the Users, Groups, Computers, or Computer Groups button.
2. Click the Search (magnifying glass) pop-up menu, choose an option to describe what you want to find, and then enter search terms in the search field.

   The original list is replaced by items that satisfy your search criteria. If you enter a user name, both full and short user names are searched. If you enter a group name, short group names are searched.
3. When the domains you're working with contain thousands of accounts, choose Workgroup Manager > Preferences and do the following:

To do this	Do this
Avoid listing accounts until a filter is specified	Select "Limit search results to requested records."
List all accounts in the selected directory domain	Enter "*" (without quotes) in the search field.
Specify the maximum number of accounts to list	Select "List a maximum of *n* records," and then enter a number no greater than 32,767.

Using Advanced Search

Use the Search button in the toolbar to locate specific users or groups by searching several fields relevant to them. You can then batch-edit these search results. For more information about batch editing, see "Editing Multiple Accounts Simultaneously" on page 48.

You can search across several fields:

- Record Name
- Real Name
- User ID
- Comment
- Keyword
- Group ID

There are several field options:

- Is less than
- Is greater than
- Is
- Contains

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

1. In the Workgroup Manager toolbar, click Search.

   You can also click the Search (magnifying glass) button in the search field above the accounts list and then choose Advanced Search.
2. Choose a field to search, a field option, and then enter the text you want to search.
3. Click the Add (+) button to add search criteria.
4. Save, rename, or delete a preset by using the Search Presets pop-up menu.
5. After you define your search, click Search Now.

   After receiving search results, you can clear the search to revert to your default display or edit the search to refine it further. While editing the search, you can save the search as a preset for later use.

Sorting Users and Groups

After displaying a list of accounts in Workgroup Manager, click a column heading to sort entries using the values in that column. Click the heading again to reverse the sort order.

Shortcuts for Working with Accounts

Workgroup Manager provides shortcuts for applying the same settings to new or existing accounts. You can also import user and group account information from a file.

Using Presets

You can select settings for a user account, group account, or computer group, and save them as presets. 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 only use presets during account creation. You can't use a preset to modify an existing account. You can use presets when creating accounts manually or when importing them from a file.

If you change a preset after it has been used to create an account, accounts already created using the preset are *not* updated to reflect those changes.

For more information about how to create presets, see "Creating a Preset for User Accounts" on page 63.

Editing Multiple Accounts Simultaneously

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

There are two ways to simultaneously edit accounts: select several accounts in the accounts list, or use the batch edit feature in the Advanced Search dialog.

Unlike when you select several accounts, the batch edit feature allows you to preview and edit search results before applying changes, and you can view changes and errors after applying more changes.

There are several ways to select multiple accounts:

- To select a range of accounts, hold down the Shift key while clicking.
- To select accounts individually, hold down the Command key while clicking.
- To deselect accounts, choose Edit > Select All and then Command-click individual accounts.

Although you can simultaneously edit most account settings for multiple users, some settings must be made for individual users. For example, you can't assign the same name, short name, or user ID to multiple users. Workgroup Manager disables fields where you must provide unique values.

If a setting is not the same for two or more accounts, you might see one of the following:

Interface element	Mixed-state appearance
Sliders, radio buttons, and checkboxes	A dash indicates that the setting is not the same for all selected accounts.
Text fields	The term "Varies" or "..." appears in the text field.
Pop-up menu	The term "--Varies--" appears in the pop-up menu.
Lists	The term "Data Varies" appears in the list.

The mixed-state interface element also appears when you do the following:

- Edit managed preferences that were originally set in Mac OS X v10.4 or earlier
- Change a preference in the preference editor that corresponds to an interface element

If you choose a new setting for a mixed-state setting, every account has the new setting.

For example, suppose you select three group accounts that 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 then have a large-size Dock.

To batch-edit accounts that match specific criteria:

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

   You can also click the magnifier in the search field above the accounts list and then choose Advanced Search.
5. To enter search criteria, choose the field to search and the field option, enter the text you want to search, and then click the Add (+) button to add additional search criteria.
6. Select "Perform a batch edit on the search results."

   You can do the following:

   - To create a list of accounts affected when you save batch edits, select "Preview and edit search results before applying changes." After editing accounts, a dialog appears listing all accounts affected by the batch edit.
   - To create a list of accounts and changes made to each account after saving batch edits, select "Display postview of changes or errors." After editing accounts, a dialog appears listing all batch edit results, uncluding the changed records and fields.

7 Click Continue.

8 Change account information or preference settings and then click Apply Now.

If a field is disabled, you can't edit the field while multiple user accounts are selected.

9 If you selected "Preview and edit search results before applying changes," you can remove accounts you don't want to batch edit by selecting them and clicking Remove.

If you perform more batch edits using the same query, removed accounts return to this list.

10 If you selected "Display postview of changes errors" and you want to save a text log of the batch-edit results, click Save and then click OK.

11 To stop batch editing, click Clear.

Importing and Exporting Account Information

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

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

Setting Up User Accounts

4

Use this chapter to set up, edit, and manage user accounts.

User accounts give users unique identities on your network and allow you to manage those users.

You can use Workgroup Manager to view, create, edit, and delete user accounts.

To view user accounts in Workgroup Manager, click the Users button above the accounts list.

About User Accounts

A user account stores data that Mac OS X Server uses to validate a user's identity and provide services to the user.

Where User Accounts Are Stored

User accounts, group accounts, computer accounts, and computer groups are stored in a directory domain, available to any Mac OS X computer. A directory domain can reside on a Mac OS X computer (for example, in an Open Directory domain or other read/write directory domain), or it can reside on a non-Apple server (for example, on a non-Apple LDAP or Active Directory server).

If you have read-only access to a directory domain, you can use augmented user records to enable specific settings or manage preferences. Because these settings are specific to the augmented records, you don't need to edit the accounts stored in the original directory domain. The settings you aren't allowed to edit are synced with the directory domain they're imported from.

For Windows file service and other services, you can store user accounts in any directory domain accessible from the server that needs to authenticate users for a service.

If the user account is used for Windows domain login from a Windows computer, you must store it in the LDAP directory of the Mac OS X Server that is the primary domain controller (PDC), or in a copy of the LDAP directory on a backup domain controller (BDC).

A Windows user account that is not stored in the PDC server's LDAP directory can be used to access other services. For example, Mac OS X Server can authenticate users with accounts in the server's local directory domain for the server's Windows file service.

Mac OS X Server also authenticates users with accounts on other directory systems, such as an Open Directory master on another Mac OS X Server system, or Active Directory on a Windows server.

For complete information about the kinds of directory domains, see *Open Directory Administration*.

Predefined User Accounts

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

Predefined user name	Short name	User ID	Use
MySQL Server	mysql	74	The user that the MySQL database server uses for its processes that handle requests.
sshd Privilege separation	sshd	75	The user for the sshd child processes that process network data.
System Administrator	root	0	A user with no protections or restrictions.

Predefined user name	Short name	User ID	Use
System Services	daemon	1	A legacy UNIX user.
Unknown User	unknown	99	A user with no login name or password. When files or volumes have no real owner, they are assigned unknown as their owner.
Unprivileged User	nobody	-2	This user was created so system services didn't need to run as System Administrator. 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

You can view, create, edit, and delete user accounts stored in various types of directory domains.

Creating User Accounts

To create a user account in a directory domain, you must have administrator privileges for the domain.

To create user accounts in an LDAPv3 directory on a non-Apple server, use Directory Utility to map the LDAPv3 directory attributes to Open Directory user and group attributes. For more information about user account elements that might need to be mapped, see "Understanding What You Can Import and Export" on page 272.

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

To create user accounts for Windows users, create them on a Mac OS X Server PDC, which creates them in the server's LDAP directory. Windows users with accounts on the PDC server can log in to the Windows domain from a Windows workstation. These user accounts can be used to authenticate to Windows file service and other services, and to Mac OS X computers on the network.

You can create user accounts in the Mac OS X Server PDC LDAP directory but not in a BDC read-only LDAP directory. If you have a BDC, the PDC server replicates the new accounts to the BDC.

If you create user accounts in a server's local directory domain, you can only authenticate for services provided by that server. You can't use these accounts to log in to a Mac OS X client computer or to perform Windows domain login. However, Windows users can authenticate with Windows file service, mail service, and other platform-neutral services.

For instructions on mapping LDAPv3 attributes or connecting to Active Directory, see *Open Directory Administration*.

To create a user account:

1. In Workgroup Manager, click Accounts.
2. Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.

   For instructions, see *Open Directory Administration*.
3. Click the globe icon and then choose the domain where you want the user's account to reside.

   For Mac OS X Server v10.5 or later, Local and /Local/Default refer to the local directory domain.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Choose Server > New User or click New User in the toolbar.
6. In the panes provided, specify settings for the user.

   For details, see "Working with Basic Settings" on page 65 through "Working with Windows Settings" on page 89.

You can also use a preset or an imported file to create a user account. For details, see "Using Presets to Create Accounts" on page 63 and "Using Workgroup Manager to Import Accounts" on page 274.

From the command line:

1. Identify an unused user ID by using the `dscl` tool to display lists of assigned user IDs and group IDs:

```
$ dscl /LDAPv3/ipaddress -list /Users UniqueID| awk '{print $2}' | sort
     -n
```

Replace */LDAPv3/ipaddress* with the location of your directory domain (the way it appears in the search path in Directory Access).

After you enter the command, the `dscl` tool displays a list of assigned user ID numbers, similar to the following output. These user IDs are for computer accounts that are included with Mac OS X Server:

```
-2
0
1
99
25
26
27
70
71
75
76
77
78
79
501
```

Important: Select a user ID that isn't in the list of assigned user ID numbers created when you install Mac OS X Server.

2 Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data, and use the `dscl` tool to create a nonadministrator user account:

```
$ dscl localhost
>
```

In interactive mode, the `dscl` tool displays the current folder in the directory domain (not the current folder in the file system) and a ">" character as a prompt.

3 Change the current folder to /LDAPv3/*ipaddress*/Users by entering the path at the prompt:

```
> cd /LDAPv3/ipaddress/Users
```

Replace *ipaddress* with the IP address of your directory server.

4 Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

5 Create a user account, replacing *ajohnson* with the new user account's short name and specifying the path to the new user's home folder in /Users/:

```
> create ajohnson HomeDirectory "<home_dir><url>afp://sp.apple.com/
    Users</url><path>ajohnson</path></home_dir>"
> create ajohnson NFSHomeDirectory /Network/Servers/sp.apple.com/Users/
    ajohnson
```

Replace `sp.apple.com` with your home folder server's location.

6 Specify the new user's default UNIX shell:

```
> create ajohnson UserShell /bin/bash
```

7 Specify the user ID, replacing *1234* with the new user's ID:

```
> create ajohnson UniqueID 1234
```

8 Specify the long name for the new user account, replacing *Anne Johnson* with the actual long name:

```
> create ajohnson RealName "Anne Johnson"
```

9 Review the settings of your new user account by entering the following command, replacing *ajohnson* with the new user account's short name as before:

```
> read ajohnson
```

10 View settings for your new user account. Settings for your new user account appear similar to the following output:

```
dsAttrTypeNative:apple-generateduid:1B2A3456-E7C8-9EC1-2345-678D912E3456
dsAttrTypeNative:cn: anne johnson
dsAttrTypeNative:gidNumber: 99
dsAttrTypeNative:HomeDirectory: /LDAPv3/ipaddress/Users/ajohnson
dsAttrTypeNative:loginShell: /bin/bash
dsAttrTypeNative:objectClass: inetOrgPerson posixAccount shadowAccount
    apple-user extensible object organizationalPerson top person
dsAttrTypeNative:sn: ajohnson
dsAttrTypeNative:uid: ajohnson
dsAttrTypeNative:uidNumber: 1234
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:1B2A3456-E7C8-9EC1-2345-678D912E3456
LastName: johnson
NFSHomeDirectory: /LDAPv3/ipaddress/Users/ajohnson
PasswordPlus:********
PrimaryGroupID: 99
RealName: Anne Johnson
RecordName: ajohnson anne
RecordType: dsRecTypeStandard:Users
UniqueID: 1234
UserShell: /bin/bash
```

11 Assign a password to the account by entering the following command, replacing *ajohnson* with the new account's short name:

```
> passwd ajohnson
```

12 Quit `dscl` by entering:

```
> quit
```

The `dscl` tool displays `Goodbye`, and then the standard shell prompt appears.

13 Use the `ssh` tool to connect to the server where you are hosting home folders:

```
$ ssh -l username server
```

Replace *username* with the name of an administrator user on the remote server and replace *server* with the name or IP address of the server.

14 Create the home folder for the new user.

Use the `-s` option if you are using a network directory domain or the `-c` option if you are using a local directory domain. You must run the command to create the home folder with root privileges.

```
$ sudo createhomedir -s -u ajohnson
```

The user account is now complete and can be used for logging in. For more information, see the `dscl` man page.

Creating Augmented User Records

Augmented user records are imported user accounts that allow you to enable specific settings such as the user's login picture, or to manage preferences. Because these settings are specific to the augmented record, you don't need to edit the accounts stored in the original directory domain.

The settings you aren't allowed to edit are synced with the directory domain they're imported from. For example, if you set a login picture for an augmented record, that augmented record uses the login picture but the original user account remains unchanged.

You can use augmented user records to manage preferences for accounts stored in an Active Directory domain or in an Open Directory domain that you don't have editing permissions for.

To create an augmented user record:

1 Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain containing the original accounts and the directory domain where the augmented user records will reside.

For instructions, see *Open Directory Administration*.

2 In Workgroup Manager, connect to the server that you're importing augmented records to.

3 Click Accounts.

4 Click the globe icon and choose the domain you're importing augmented records to.

5 To authenticate, click the lock and enter the name and password of a directory administrator of the directory domain you chose in the previous step.

6 Choose Server > New Augmented User Records.

7 Select the user records you want to import.

If you select a group, all members of that group are imported.

8 Click Create, and then click Done.

Editing User Account Information

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

You can modify accounts in an Open Directory domain if you're authorized to administer the directory domain. You don't need server administrator privileges but your user ID must have limited or full administrative privileges (which are set in the Privileges pane of Accounts in Workgroup Manager). For more information, see "Working with Privileges" on page 73.

To make changes to a user account:

1 In Workgroup Manager, click Accounts.

2 Make sure that the directory services of the Mac OS X Server computer you're using are configured to access the desired directory domain.

For instructions, see *Open Directory Administration*.

3 Click the globe icon and then choose the domain where the user's account resides.

If the directory domain is not listed, add it to the pop-up menu by choosing Other. In the dialog that appears, select the domain and then click OK.

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

5 Click the Users button and select the user account.

6 In the panes provided, edit settings for the user account.

For details, see "Working with Basic Settings" on page 65 through "Working with Windows Settings" on page 89.

Editing User Account Information from the Command Line

You can set or modify the following user account attributes using `dscl`:

Attribute	Description
apple-GeneratedUID	User ID generated by the system
cn	User's common name
homeDirectory	Location of the user's home folder
loginShell	User's Terminal shell
sn	User's surname
LastName	User's last name
NFSHomeDirectory	Location of the user's Home folder
PrimaryGroupID	User's primary group ID
RealName	User's name
UserShell	User's Terminal shell

To change a user account attribute to a new value:

1. Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

```
$ dscl localhost
>
```

2. Change the current folder to

```
> cd /LDAPv3/ipaddress/Users
```

Replace *ipaddress* with the IP address of your directory server.

3. Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

4. Set the user attribute to the desired value by entering the following command:

```
> create ajohnson attribute newvalue
```

Replace *ajohnson* with the user account's short name, *attribute* with the name of the attribute whose value you want to change, and *newvalue* with the value.

5. Quit `dscl` by entering:

```
> quit
```

Working with Read-Only User Accounts

Use Workgroup Manager to review information about 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 Make sure that the directory services of the Mac OS X Server computer you're using are configured to access the directory domain where the account resides.

For information about using Directory Utility to configure server connections, see *Open Directory Administration*. For information about the user account elements that need to be mapped, see the appendix, "Importing and Exporting Account Information."

3 Click the globe icon and choose the directory domain where the user's account resides.

4 Review the user's account settings using the panes provided.

For details, see "Working with Basic Settings" on page 65 through "Working with Windows Settings" on page 89.

Working with Guest Users

You can set up some services to support guest users, who are not authenticated because they don't have a valid user name or password. You don't need to create a user account to support guest users.

The following services can be set up to support guest access:

- **Apple file service.** See *File Server Administration*.
- **FTP service.** See *File Server Administration*.
- **Web service.** See *Web Technologies Administration*.
- **Windows services.** See *Open Directory Administration*.

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

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

Working with Windows User Accounts

Use Workgroup Manager to change passwords, password policies, and other settings in Windows user accounts.

The user accounts can reside in a server's local directory domain, a Mac OS X Server PDC LDAP directory, or another directory system that allows read-write access (not read-only access) such as an Open Directory master LDAP directory or Active Directory on a Windows server.

You can change the user account settings in the Mac OS X Server PDC LDAP directory but not in a BDC read-only LDAP directory. If you have a BDC, the PDC server replicates the changes to the BDC.

Deleting a User Account

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

> *WARNING:* You cannot undo this action.

Deleting a user account also deletes all of the user's mail.

To delete a user account using Workgroup Manager:

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

From the command line:

1. Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

   ```
   $ dscl localhost
   >
   ```

2. Change the current folder to /LDAPv3/*ipaddress*/Users by entering the path at the prompt:

   ```
   > cd /LDAPv3/ipaddress/Users
   ```

   Replace *ipaddress* with the IP address of your directory server.

3. Authenticate as an administrator by entering the following command, replacing *adminusername* with an administrator's user name, and entering that administrator's password when prompted:

   ```
   > auth adminusername
   ```

4. Delete the user account by entering the following command, replacing *ajohnson* with the user account's short name:

   ```
   > delete ajohnson
   ```

5. Quit `dscl` by entering:

   ```
   > quit
   ```

Disabling a User Account

To disable a user account, you can:

- Deselect the "User can access account" option in the Basic pane in Workgroup Manager.
- Delete the account.
- Change the user's password to an unknown value.

- Set password options to disable login. This applies to user accounts with the password type Open Directory or Shadow Password.

To disable a user account using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to delete.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. In the Basic pane, deselect "User can access account" and click Save.

From the command line:

1. Disable the user account:

```
$ pwpolicy -a diradmin -u ajohnson -setpolicy "isDisabled=1"
```

Replace *ajohnson* with the short name of the user account. Replace *diradmin* with the short name of your directory administrator account.

Note: The `pwpolicy` command only works for LDAP/Password server users. For a local user, use Workgroup Manager or the Accounts pane of System Preferences.

2. Kill the user's active processes that are running on the directory server:

```
$ sudo killall -TERM -u ajohnson
```

Replace *ajohnson* with the user name.

3. Wait a few seconds to allow the previous command to execute; then, terminate the user's processes:

```
$ sudo killall -9 -u ajohnson
```

Replace *ajohnson* with the user name.

For more information about terminating processes, see the `killall` man page.

To reenable a user account using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Select the user account you want to delete.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. In the Basic pane, select "User can access account" and click Save.

From the command line:

- Enable a disabled user account:

```
$ pwpolicy -a diradmin -u ajohnson -setpolicy "isDisabled=0"
```

Replace *ajohnson* with the short name of the user account. Replace *diradmin* with the short name of your directory administrator account.

Working with Presets

Presets are templates used to define attributes that apply to new user, group, or computer group accounts.

Creating a Preset for User Accounts

You can create presets to use when creating user accounts in a directory domain.

Presets are stored in the directory domain you're currently viewing. If you change directory domains, the presets you created in the other directory domain are not available.

To create a preset for user accounts:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the domain where the user's account resides.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. To create a preset using data in an existing user account, open the account; to create a preset from scratch, create a user account.
5. If you're basing the preset on an existing account, fill in the fields with values you want new user accounts to inherit and then delete values you don't want to specify in advance.

   The following attributes can be defined in a user-account preset: simultaneous login, default shell, comment, primary group ID, group membership list, home folder settings, disk quota, mail settings, and print settings.
6. Click Preferences.
7. Configure settings you want the preset to define and then click Accounts.

   After configuring preference settings for a preset, you return to the Accounts settings to save the preset.
8. From the Presets pop-up menu, choose Save Preset, enter a name for the preset, and click OK.

   The preset is saved to the current directory domain.

Using Presets to Create Accounts

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

You can use presets with user, group, and computer group accounts.

Presets are stored in the directory domain you're viewing. If you change directory domains, the presets you created in the other directory domain are not available.

When importing accounts, you can apply a preset to the imported account. For more information, see "Using Workgroup Manager to Import Accounts" on page 274.

To create an account using a preset:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and then choose the directory domain where you want the new account to reside.

   Make sure the directory domain you choose contains the preset you want to use.
3. To authenticate, click the lock and then enter the name and password of a directory administrator.
4. Click the Users, Groups, or Computer Groups button.
5. From the Presets pop-up menu, choose a preset.
6. To create accounts, click New User, New Group, or New Computer Group.
7. Add or update attribute values.

Renaming Presets

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

To rename a preset:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and then choose the directory domain that has the preset you want to rename.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. From the Presets pop-up menu, choose Rename Preset.
5. Choose a preset from the "Rename preset" pop-up menu, enter a name, and then click OK.

Editing Presets

When you change a preset, existing accounts that were created with it are not updated to reflect the changes.

You edit a preset by using it to create an account, changing fields defined by the preset, and then saving the preset.

To edit a preset:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the directory domain with the preset you want to edit.

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

4 Click the Users, Groups, or Computer Groups button.

5 From the Presets pop-up menu, choose a preset.

6 Click New User, New Group, or New Computer Group to create accounts.

7 Change account settings that you want to save to the preset.

8 After completing your changes, choose Save Preset from the Presets pop-up menu, enter the name of the preset you want to change, click OK, and then click Replace.

Deleting a Preset

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

To delete a preset:

1 In Workgroup Manager, click Accounts.

2 Click the globe icon and choose the directory domain with the preset you want to delete.

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

4 From the Presets pop-up menu, choose Delete Preset.

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

Working with Basic Settings

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

In Workgroup Manager, use the user account's Basic pane to work with basic settings.

Modifying User Names

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

A user name can contain no more than 255 bytes. Because long user names support various character sets, the maximum number of characters for long user names ranges from 255 Roman characters to as few as 63 characters in character sets where characters occupy up to 4 bytes.

Use Workgroup Manager to edit the user name of an account stored in an Open Directory domain, the local directory 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 user account you want to work with.

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

   Initially, the value of the user name is "Untitled #," where # is the sequential number generated after the last generated number for an existing untitled user.

   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 domain or in a domain in the search policy. However, it can't detect whether duplicates exist in other domains.

Modifying Short Names

A *short name* is an abbreviated name for a user, such as "mchen" or "annejohnson." Users can log in using a short name or the user name associated with his or her accounts. The short name is used by Mac OS X for home folders.

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

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

For the first short user name, use only these characters. Subsequent short names can contain any Roman character.

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

Typically, short names contain eight or fewer characters.

Initially, the value of the first short name is "untitled_#," where # is the sequential number generated after the last generated number for an existing untitled user.

Avoid assigning the same name to more than one user. Workgroup Manager doesn't let you assign the same name to different users in a domain or in a domain search policy. However, it can't detect whether duplicates exist in other domains.

After the user's account is saved you can't change the first short name but you can change any of the other short names.

Use Workgroup Manager to edit the short name of an account stored in an Open Directory domain, the local directory 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 short name using Workgroup Manager:

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

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

To do this	Do this
Change a short name	Double-click the short name and then replace it.
Add a short name	Double-click the blank entry at the bottom of the short name list and then enter a short name.

Choosing Stable Short Names

When you create a user account, assign the account a short name that won't be changed. After creating the account, you can't use the Basic pane of Workgroup Manager to change a user's first short name.

To change a user's first short name, create an account for the user in the same directory domain that contains the new first short name and retain all other account information (user ID, primary group, home folder, and so on). Make sure you use the same GUID for the new account. Then disable the login for the old user account.

After you disable the old login, the user can log in using the changed name but will have the same access to files and other network resources as before and will belong to the same groups.

For more information, see "Working with GUIDs" on page 91, and"Disabling a User Account" on page 61.

Avoiding Duplicate Names

A user's short name is used by the login window. This means that having multiple users with the same short name causes a conflict. Although you can't create multiple users with the same short name in the Basic pane of Workgroup Manager, it's still possible to create multiple users with the same short name when you use command-line tools or the Inspector.

If multiple user accounts have the same long user name on a Mac OS X computer, the login window displays a list of users to choose from.

If two users have the same first short user name, the login window only recognizes and authenticates the first matching user account it finds in the sequence of directory domains specified by the computer's search policy, as set in Directory Utility.

If a local user and a network user have the same first short user name, the local user always takes precedence, preventing the network user from logging in to the computer.

In groups created using Mac OS X versions earlier than 10.4, group membership is determined by the user's first short name and group ID (GID). If multiple users have the same first short name, they have the same group memberships.

Groups created using Mac OS X Server v10.4 or later determine group membership using a GUID and a combination of the user's short name and GID. For information about GUIDs, see "Working with GUIDs" on page 91.

If you don't upgrade legacy groups, the groups still determine membership by only the user's first short name and GID. For instructions on upgrading legacy groups, see "Upgrading Legacy Groups" on page 101.

To ensure that users have the correct legacy group membership, do not use duplicate user short names.

To see if names are in use from the command line:

- To see if a short name is in use:

  ```
  $ id shortname
  ```

  The command searches all connected directories and lists users with the shortname.

- To get the default UNIX short name for a user long name:

  ```
  $ sudo /System/Library/ServerSetup/serversetup -getUNIXName "longname"
  ```

  Note: Mac OS X Server provides the `net` tool, which is essentially a clone of the Windows `net` command. The `net` tool enables administrators to perform advanced customization of the Primary Domain Controller (PDC) and mapping domain privileges to UNIX groups. For more information, see the `net` man page.

- To view a user's account information:

```
$ dscacheutil -q user -a name jdoe
name: jdoe
password: ********
uid: 501
gid: 501
dir: /Users/jdoe
shell: /bin/csh
gecos: John Doe
```

- To view all user accounts:

```
$ dscacheutil -q user
```

For more information about `dscacheutil`, see its man page.

Modifying User IDs

A *user ID* is a number that uniquely identifies a user. Mac OS X computers use the user ID to track a user's folder and file ownership.

When a user creates a folder or file, the user ID is stored as the ID of the user who created the folder or file. This user ID has read and write permissions to the folder or file by default.

The user ID should be a unique string of digits from 500 through 2,147,483,647. It is risky to assign the same user ID to different users, because two users with the same user ID have identical directory and file permissions.

User IDs between 0 and 100 are reserved for system use and should not be deleted or modified except to change the password of the root user. Accounts with user IDs below 100 aren't listed in the login window.

In general, after user IDs are assigned and users start creating files and folders, you shouldn't change user IDs. However, one possible scenario where you might need to change a user ID is when merging users that were created on different servers onto a new server or cluster of servers. The same user ID might still be associated with a different user on the previous server.

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

You can use Workgroup Manager to edit the user ID of an account stored in an Open Directory domain or in the local directory 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 user account you want to work with.

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

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

   You can quickly find all existing user IDs by choosing View > "Show System Users and Groups," and then clicking the UID column header in the accounts list to sort the accounts by user ID.

To see if a user ID is in use from the command line:

```
$ sudo /System/Library/ServerSetup/serversetup -verifyUID uid
```

The command displays a `1` if the UID is in use, or a `0` if it isn't.

To view names associated with a user ID is in use from the command line:

```
$ sudo /System/Library/ServerSetup/serversetup -getNamesByID uid
```

If you don't receive a response, the UID is not valid.

Assigning a Password to a User

When you create a user account, you must assign a password to the user. You can reset the user's password by replacing the password field with a new password.

For information about choosing secure passwords, see *Mac OS X Security Configuration*.

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

For more information about importing user accounts, see "Understanding What You Can Import and Export" on page 272.

To assign a password:

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

   To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.

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

4 In the Basic pane, enter a password in the Password field, enter it again in the Verify field, and then click Save.

To test a user's password from the command line

```
$ sudo /System/Library/ServerSetup/serversetup -verifyNamePassword
     shortname password
```

The command displays a `1` if the password is good, or a `0` if it isn't.

Assigning Administrator Privileges for a Server

A user who has server administrator privileges controls most of the server's configuration settings and can use applications (such as Server Admin) that require a user to be a member of the server's administrator group.

You can use Workgroup Manager to assign server administrator privileges to a user with an account stored in an Open Directory 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 you want to grant administrator privileges for.

2 Click Accounts.

3 Click the globe icon and choose Local.

4 Click the lock and enter the name and password of a local administrator.

5 Click the globe icon and choose the directory domain where the user's account resides.

6 Click the lock and enter the name and password of a directory administrator.

7 Select a user account.

8 In the Basic pane, select "User can administer this server."

From the command line:

- To create a local administrator user account:

  ```
  $ sudo /System/Library/ServerSetup/serversetup -createUser fullname
     shortname password
  ```

  Enter the name, short name, and password in the order shown. If the full name includes spaces, enter it in quotes.

  The command displays a `0` if successful, or a `1` if the full name or short name is already in use.

- To create a local administrator user with a specific UID:

```
$ sudo /System/Library/ServerSetup/serversetup -createUserWithID
   fullname shortname password uid
```

Enter the name, short name, password, and UID in the order shown. If the full name includes spaces, enter it in quotes.

The command displays a `0` if successful, or a `1` if the full name, short name, or UID is already in use or if the UID you specified is less than 100.

- To create a local administrator user with a specific UID and home folder:

```
$ sudo /System/Library/ServerSetup/serversetup -createUserWithIDIP
   fullname shortname password uid homedirpath
```

Enter the name, short name, password, and UID in the order shown. If the full name includes spaces, enter it in quotes.

The command displays a `0` if successful, or a `1` if the full name, short name, or UID is already in use or if the UID you specified is less than 100.

- To see if a user is a server administrator:

```
$ sudo /System/Library/ServerSetup/serversetup -isAdministrator
   [shortname]
```

The command displays a `0` if the user is an administrator, or a `1` if the user is not an administrator.

Choosing a User's Login Picture

You can change a user's login picture using Workgroup Manager. This picture represents the user in the login window, in the Directory application, and in group web services, and is the default buddy icon for the user in iChat.

Although you can use an image file of any size, you should use an image that is 64x64 pixels in size. If you use a larger image, resize and crop it in Workgroup Manager.

To change a user's login picture:

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

   To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. In the Basic pane, click the picture area in the top right and then choose Edit Picture to open the User Picture window.
5. In the User Picture window, click Choose, select an image file, and then click Open.

   As an alternative, you can drag an image file from the Finder or Safari and drop it into the picture area in Workgroup Manager, or in the main area of the User Picture window.

If you have iSight, you can click the camera button to take a snapshot.

6 Use the slider to zoom in and out of your picture and drag your picture around so the focal point is in the center square, and then click Set.

The user's picture is the image in the center square.

7 Click Save.

Working with Privileges

You can give a user account full or limited control over domain administration. When giving limited administrative control, you can choose which users and groups the user can administer, and what kind of control the user has over those users and groups.

You can change a user's domain privileges for Open Directory domains. You can't change privileges for a local user account or an account stored in domains that are not Open Directory.

Full and limited administrators use Workgroup Manager to administer and manage users.

In Workgroup Manager, use the user account's Privileges pane to set privileges.

Removing Administrative Privileges from a User

Users with no administrative privileges can use Workgroup Manager to view (but not change) accounts in a directory domain.

You can change a user's domain privileges for LDAPv3 directory domains. You can't change privileges for a local user account or an account stored in a non-LDAPv3 directory domain.

To remove a user's administrative privileges:

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.

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

4 In Privileges, choose None from the "Administration capabilities" pop-up menu and click Save.

Giving a User Limited Administrative Capabilities

You can allow users who don't need full administrative control the ability to perform common administrative tasks by giving them limited administrative control.

For example, you might want student lab assistants to reset other students' passwords but not to edit the groups they belong to. Similarly, you might want school staff to edit student user information but not their managed preferences.

When a user has limited administrative control, after authenticating in Workgroup Manager, the Workgroup Manager interface only allows users to perform tasks assigned to the limited administrator.

The following tasks are available to limited administrators:

Task	Description
Manage user passwords	Change a user's password in the user account's Basic pane. A limited administrator can't change a full administrator's password.
Edit managed preferences	Change managed preference settings.
Edit user information	Edit the user account's Info pane.
Edit group membership	Edit the user account's Groups pane or the group account's Members pane.

If you give a user different administrative capabilities at several account levels, the capabilities are merged.

For example, let's say a user named Anne Johnson is a member of the Algebra 101 group, and the Algebra 101 group is a member of the All Classes group. You give another user, Ravi Patel, the following administrative control:

- "Manage user passwords" rights for All Users and Groups
- "Edit managed preferences" rights for the All Classes group
- "Edit user information" rights for the Algebra 101 group
- "Edit group membership" rights for the Anne Johnson user account

Ravi Patel has all four abilities for Anne Johnson's user account.

You can change a user's domain privileges for LDAPv3 directory domains. You can't change privileges for a local user account or an account stored in a non-LDAPv3 directory domain.

To add limited administrative capabilities:

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

   To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.
3. To authenticate, click the lock and enter the name and password of a directory administrator.

4 In Privileges, choose Limited from the "Administration capabilities" pop-up menu.

5 To control the level of user or group administration, click the Add (+) button and drag users and groups from the drawer to the "User can administer" list.

6 Select a user or group from the "User can administer" list and then select the administration capabilities you want the limited administrator to have.

To give administrative control to all users and groups, select "All Users and Groups" and then select administrative capabilities.

7 Click Save.

Giving a User Full Administrative Capabilities

A user with full administrative capabilities is also known as a *directory administrator.* Directory administrators can modify any records in the directory domain and are the only users who can change the passwords of other directory administrators.

You can change a user's domain privileges for LDAPv3 directory domains. You can't change privileges for a local user account or an account stored in a non-LDAPv3 directory domain.

To change a user's administrative privileges:

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.

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

4 In Privileges, from the "Administration capabilities" pop-up menu, choose Full, and then click Save.

From the command line:

1 Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data.

Use the `dscl` tool to create a directory administrator user account.

```
$ dscl localhost
>
```

In interactive mode, the `dscl` tool displays the current folder in the directory domain (not the current folder in the file system) and a ">" character as a prompt.

2 After you connect to the directory, choose the directory domain and change the current folder to LDAPv3/*ipaddress*/Groups:

```
> cd LDAPv3/ipaddress/Groups
```

Replace *`ipaddress`* with the IP address of your directory server.

3 Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

4 Create an administrator user.

```
> append admin Member adminusername
```

This command creates an administrator user, but it doesn't add the globally unique identifier (GUID) of the administrator user to the group account.

5 Add the administrator user to the group.

```
> append admin GroupMembers guid
```

Replace *guid* with the globally unique identifier.

6 Quit the `dscl` tool.

```
> quit
```

Working with Advanced Settings

Advanced settings include login settings, keywords, password type, and searchable comments. In Workgroup Manager, use the user account's Advanced pane to work with advanced settings.

Enabling a User's Calendar

If you connect to a server running Mac OS X Server v10.5 and iCal service with individual user calendars enabled, you can configure user accounts to use iCal server. When users use iCal to log into the server, they can access their calendars.

If you connect to a server running Mac OS X Server v10.6 or later, use iCal Service Utility to configure user calendars.

To enable a user's calendar:

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

To select an account, click the globe icon above the accounts list, choose the directory domain where the user's account resides, and then select the user.

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

4 In Advanced, select "Enable calendaring," choose a server from the pop-up menu, and then click Save.

Allowing a User to Log In to More Than One Computer at a Time

You can allow a managed user to log in to more than one managed computer at a time, or you can prevent the user from doing so.

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

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

To allow a user to log in to more than one computer at a time:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Advanced.
5. Select "Allow simultaneous login on managed computers."

Choosing a Default Shell

You can change the default shell that the user uses for command-line interactions with Mac OS X, such as /bin/tcsh or /bin/bash (the default).

The default shell is used by the Terminal application on the computer that the user is logged in to, but Terminal has a preference that lets you override the default shell. The default shell is used by secure shell (SSH) when the user logs in to a remote Mac OS X computer.

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

To choose a default shell:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. To specify the user's default shell when logging in to a Mac OS X computer, choose a shell from the Login Shell pop-up menu.

   To specify a shell that doesn't appear in the list, choose Custom and then enter the path to the shell.

To ensure that a user can't access the server remotely using the command line, choose None.

Choosing a Password Type and Setting Password Options

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

When you set the password type to Shadow Password or Open Directory, you can set several password policy options, including disabling login after a period of inactivity or failed authentication attempts, or setting password restrictions (such as requiring that passwords have a specific minimum length or that they be changed at the next login).

If you set the password type to Shadow Password, you can also set security options to control which authentication methods are used when validating the user's password.

You can only assign the Open Directory password type if the directory administrator account that you authenticate with also uses an Open Directory password.

Windows users must have Open Directory passwords for Windows domain login.

For a detailed explanation of password types, password policy options, and security options, see *Open Directory Administration*.

To choose a user password type and set password options:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Advanced.
5. From the User Password Type pop-up menu, choose Shadow Password, Open Directory, or Crypt Password.

   When you choose a password type, a prompt might appear requiring you to enter a password, depending on whether you entered a password in the Basic pane.

   If you choose Open Directory or Shadow Password, you can set a password policy for the selected users by clicking Options, selecting any of the options, and clicking OK.

   If you choose Shadow Password, you can also select authentication methods by clicking Security.
6. Click Save.

Creating a Master List of Keywords

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

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

Each directory domain has its own master keyword list. For example, if you add a keyword to the local directory domain's master keyword list, it isn't available in another directory domain unless you add it to that directory domain's master keyword list.

To edit the master keyword list:

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

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

To do this	Do this
View the master keyword list, which lists all terms available for use as keywords	Click the Edit (pencil) button. You can access and edit the master keyword list from any selected user account.
Add a keyword to the master list	Click the Add (+) button and enter the keyword in the text field.
Remove a keyword from the master list and from user and computer accounts where it appears	Select the keyword, select "Remove deleted keywords from users and computers," and then click the Remove (–) button.
Remove a keyword only from the master list	Deselect "Remove deleted keywords from users and computers," select the keyword you want to remove, and then click the Remove (–) button.

5. When you finish editing the master list, click OK.

Applying Keywords to User Accounts

You can remove a keyword from all user accounts that are tagged with that keyword. However, you can only add keywords to one user account at a time.

To work with keywords for a user account:

1. In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Advanced and choose from the following:

To do this	Do this
Add a keyword to the account	Click the Add (+) button to view the list of available keywords, select keywords in the list, and then click OK.
Remove a keyword from the account	Select the keyword you want to remove and click the Remove (–) button.

5 When you finish adding or removing keywords for the user account, click Save.

Editing Comments

You can save a comment in a user's account to provide information you might need to help administer a user. A comment can contain no more than 32,767 bytes.

Note: Some character sets use characters that occupy up to 4 bytes. This reduces the total number of characters you can use.

You can use Workgroup Manager to add a comment to an account stored in an Open Directory domain, the local directory 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 user account you want to work with.

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

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

4 Click Advanced and edit or review the contents of the Comment field.

Working with Group Settings

Group settings identify the groups a user belongs to. In Workgroup Manager, use the Group Settings pane in the user's account to work with group settings.

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

Choosing a User's Primary Group

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

Important: Don't rely on primary group membership when assigning file permissions. Although you can make a primary group a hierarchical group or a parent of hierarchical groups, the file permissions for the primary group do not propagate. If a user's primary group is a hierarchical group or the parent of a hierarchical group, the user is granted file permissions only for the primary group.

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

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

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

To set a primary group ID using Workgroup Manager:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Groups and then edit or review the Primary Group ID field.

   Workgroup Manager displays long and short names for the group after you enter a primary group ID (if the group exists and is accessible in the search policy of the server you're logged in to).

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.

You can view all groups the user belongs to and the parent groups of those groups.

To review group memberships using Workgroup Manager:

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

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

   Except for the primary group, all other groups the user belongs to are listed in the Other Groups list.
5. To view parent groups, click Show Inherited Groups.

   Parent groups are shown in italics.

Adding a User to a Group

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

For example, you can have groups for students in a classroom who are not permitted to use a specified printer, or for the quality control team in a factory that requires access to the internal reports of different groups.

Groups can include users and groups that are in an Open Directory domain or the local directory domain. If you use an NFS directory, there is a 16-group limitation.

You can also add users to a group using the Members pane in the group account.

If a user is a direct member of multiple groups, he or she can choose which group to acquire managed preferences from when logging in. You can manage Login preferences so that preferences are combined from all workgroups accessible by the user.

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

To add a user to a group using Workgroup Manager:

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

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

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

4 Click Groups and then click the Add (+) button.

This opens a drawer that lists the groups defined in the directory domain you're working with.

5 Select the group and then drag it to the Other Groups list in the Groups pane.

For information about adding users and groups to groups using the command line, see "Adding Users or Groups to a Group" on page 106.

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 an Open Directory domain or the local directory domain.

To remove a user from a group using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Groups.

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

You can also remove users from a group by using the Members pane of group accounts. For more information, see "Removing Group Members" on page 108.

Working with Home Settings

Home settings describe a user's home folder attributes. If you don't have a share point set up to host home folders, you must set one up. To set up share points, use Server Admin. To set up home folders, use Workgroup Manager.

For information about setting up share points and home folders, see Chapter 7, "Setting Up Home Folders."

Working with Mail Settings

You can create a mail account by specifying mail settings in the user account. To use the mail service 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 to work with mail settings.

For information about how to set up and manage Mac OS X Server mail service, see *Mail Server Administration*.

Enabling Mail Service Account Options

You can use Workgroup Manager to enable mail service and set mail options for a user account stored in an Open Directory domain or other read/write directory domain. You can also use Workgroup Manager to review the mail settings of accounts stored in a 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 user account you want to work with.

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Mail.
5. To allow the user to use mail service, select Enabled.
6. In the Mail Server field, enter a valid mail server name or address for the DNS name, or enter the IP address of the user's mail server.

   Workgroup Manager doesn't verify this information.
7. In the Mail Quota field, enter a value to specify the maximum number of megabytes for the user's mailbox.

   A 0 (zero) or empty value means no quota is used.

   When the user's message space approaches or surpasses the mail quota you specify, mail service displays a message prompting the user to delete unwanted messages to free up space. The message shows quota information in megabytes (MB).
8. To identify the protocol used for the user's mail account, select a Mail Access setting: Post Office Protocol (POP), Internet Message Access Protocol (IMAP), or both.
9. Click Save.

Disabling a User's Mail Service

You can use Workgroup Manager to disable mail service for users whose accounts are stored in an Open Directory domain, the local directory 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 user account you want to work with.

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

Forwarding a User's Mail

You can use Workgroup Manager to set up mail forwarding for users whose accounts are stored in an Open Directory domain or the local directory domain.

To forward a user's mail using Workgroup Manager:

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

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

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

Working with Print Quota Settings

User print settings define the ability of a user to print to accessible Mac OS X Server print queues.

For information about how to set up print queues, see *Print Server Administration*.

In Workgroup Manager, use the Print Quota pane in the user account to work with print quota settings.

Enabling a User's Access to All Available Print Queues

You can use Workgroup Manager to allow a user to print to all accessible Mac OS X print queues that enforce quotas. To use Workgroup Manager to enable access to print queues, the user's account must be stored in an Open Directory domain or the local directory domain.

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

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. In Print Quota, select "All Queues."
5. Enter values for the maximum number of pages the user can print in a specific number of days.

   For the settings to take effect, the print queue must enforce quotas.
6. Click Save.

Enabling a User's Access to Specific Print Queues

You can use Workgroup Manager to allow a user to print to specific accessible Mac OS X print queues that enforce quotas. To use Workgroup Manager to enable access to print queues, the user's account must be stored in an Open Directory domain or the local directory domain.

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

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. In Print Quota, select "Per Queue."
5. If the print queue you want to specify is not on the Queue Name pop-up menu, click Add, enter the queue name, and then specify the IP address or DNS name of the server where the queue is defined in the Print Server field.

   For your settings to take effect, the print queue must enforce quotas.

6 To give the user unlimited printing rights to the queue, select "Unlimited printing"; otherwise, select "Limit to" and specify the maximum number of pages the user can print in a specific number of days.

7 Click Save.

Removing a Print Quota for a Queue

If you no longer require a print quota for a queue, you can use Workgroup Manager to delete the quota for specific users.

To delete specific print quotas, you must manage print settings per queue.

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

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Print Quota and then select Per Queue.

5 Choose the user's print queue that you want to delete from the Queue Name pop-up menu.

6 Click Delete and then click Save.

Resetting a User's Print Quota

Occasionally, a user exceeds his or her print quota and needs to print additional pages. For example, an administrator might want to print a 200-page manual, but the print quota is only 150 pages. Or a student might exceed his or her quota by printing several revisions of the same essay.

You can use Workgroup Manager to reset a user's print quota and allow the user to continue printing.

You can also extend a user's page limit without resetting the quota 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 current and future print quota periods.

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

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Print Quota.

5 If you're managing All Queues, click Restart Print Quota.

6 If you're managing Per Queue, choose a print queue from the Queue Name pop-up menu and then click Restart Print Quota.

7 To increase or decrease a user's page limit, enter a new number in the "Limit to ___ pages" field.

8 Click Save.

Disabling a User's Access to Print Queues That Enforce Quotas

You can use Workgroup Manager to prevent a user from printing to any accessible Mac OS X print queues that enforce quotas.

To use Workgroup Manager to disable access to print queues, the user's account must be stored in an Open Directory domain or the local directory domain.

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

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Print Quota and then select None.

Working with Info Settings

If a user's account resides in an LDAPv3 directory domain, it can contain information imported from Address Book.

Attributes that are tracked in the Info pane include:

- Name
- Address
- Phone number
- Email address
- Chat names
- Homepage URL
- Weblog URL

Other users can view the information in this pane when they view the user account in Workgroup Manager and Directory.

To change a user's info:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, and then select the user account in the accounts list.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Info, enter or change values, and when you finish, click Save.

Working with Windows Settings

Windows users have settings for a Windows home folder, a roaming user profile, and a Windows login script. You can change these settings in the Windows pane of Workgroup Manager.

You can change user account settings in the Mac OS X Server PDC LDAP directory but not in a BDC read-only LDAP directory. If you have a BDC, the PDC server replicates changes to the BDC.

Changing a Windows User's Profile Location

You can change where a Windows user's profile settings are stored. The profile includes the user's My Documents folder, favorites (web browser bookmarks), preference settings (such as backgrounds and event sounds), and more.

User profiles are stored in /Users/Profiles/ on the PDC server. This is an SMB share point, although it is not shown as a share point in Workgroup Manager.

You can designate a different location for a user profile, which can be a share point on the PDC server or a Windows domain member server. The share point must be configured to use SMB.

User profiles can be located in a share point or in a folder in a share point. The share point or folder used for user profiles must have the proper access privileges.

Set the owner to "root" and give the owner Read & Write permission. Set the group to the user's primary group (which is normally "staff") and give the group Read & Write permission. Set the permission for everyone else to None.

For instructions, see "Setting Up an SMB Share Point" on page 129.

Instead of storing a roaming profile in a share point on a server, you can designate the location of a local profile stored on the Windows computer.

To change the Windows roaming profile location for a user account:

1. In Workgroup Manager, click Accounts.
2. Open the user account whose profile location you want to change.

   To open a user account in the PDC, click the globe icon and choose the PDC server's LDAP directory.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Windows and enter the new profile location in the User Profile Path field.
   - To use the default share point for user profiles, leave this field blank.
   - For a roaming profile stored in a different share point, enter the location of the share point using the universal naming convention (UNC) format:

     *servername**sharename**usershortname*

     For *servername,* substitute the NetBIOS name of the PDC server or a Windows domain member server where the share point is located.

     To view the server's NetBIOS name, open Server Admin, select SMB in the Servers list, click Settings, click General, and then look at the Computer Name field.

     For *sharename,* substitute the name of the share point.

     For *usershortname,* substitute the first short name of the user account you're configuring.
   - For a local profile stored on the Windows computer, enter the drive letter and folder path in UNC format as in the following example:

     C:\Documents and Settings\juan
5. Click Save.

Changing a Windows User's Login Script Location

You can use Workgroup Manager to change the folder location of a user's Windows login script in the /etc/netlogon/ folder on the PDC server.

To change the Windows login script location for a user account:

1. In Workgroup Manager, click Accounts.
2. Open the user account whose Windows login script location you want to change.

   To open a user account in the PDC, click the globe icon and choose the PDC server's LDAP directory.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Windows and enter the new login script location in the Login Script field.

Enter the relative path to a login script in /etc/netlogon/ on the PDC server. For example, if an administrator places a script named setup.bat in /etc/netlogon/, the Login Script field should contain "setup.bat."

5 Click Save.

Changing a Windows User's Home Folder Drive Letter

You can use Workgroup Manager to change the Windows drive letter that a user's home folder is mapped to.

To change the Windows home folder drive letter for a user account:

1 In Workgroup Manager, click Accounts.

2 Open the user account whose Windows home folder drive letter you want to change.

To open a user account in the PDC, click the globe icon and choose the PDC server's LDAP directory.

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

4 Click Windows and choose a drive letter from the Hard Drive pop-up menu.

The default drive letter is H. Windows uses the drive letter to identify the mounted home folder.

5 Click Save.

Changing a Windows User's Home Folder Location

You can change where a Windows user's network home folder is stored. By default, the network home folder is the same for Windows as it is for Mac OS X, and its location is specified in the Home pane.

For more information, see "Setting Up a Home Folder for a Windows User" on page 137.

Working with GUIDs

Although you can view and modify most user account attributes using the Accounts pane in Workgroup Manager, you must use the Inspector to view and modify GUIDs.

Viewing GUIDs

GUIDs are stored in the directory domain and are not immediately visible in Workgroup Manager. To view GUIDs, you must first enable the Inspector in Workgroup Manager. For instructions on using the Inspector, see *Open Directory Administration*.

> ***WARNING:*** Although the Inspector allows you to edit GUIDs, it is not recommended. Doing so destroys existing group memberships and file permissions for that user ID.

To view a user or group GUID:

1. In Workgroup Manager, click Accounts.
2. Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.
3. Click the globe icon and then choose the domain where the account resides.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Click the Users, Groups, Computers, or Computer Groups button and select the account.

   You can only view GUIDs for individual accounts.
6. Click the Inspector button under the lock at the far right.

   If there is no Inspector button, make sure the Inspector is enabled by choosing Workgroup Manager > Preferences, and then select "Show "All Records' tab and inspector."
7. Select the GeneratedUID field and then click Edit.
8. Click Cancel to make sure you do not change the GUID.

From the command line:

- `$ dscl /Search -read /Users/username GeneratedUID`

Setting Up Group Accounts

5

Use this chapter to set up, edit, and manage group accounts.

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

You can use Workgroup Manager to view, create, edit, and delete group accounts.

To view group accounts in Workgroup Manager, click the Groups button above the accounts list.

About Group Accounts

A group account stores the identities of users who belong to the group, as well as information that lets you customize the working environment for members of the group. When you define preferences for a group, the group is known as a *workgroup*.

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

How Group Accounts Track Membership

Mac OS X Server uses GUIDs and a combination of the user's short name and GID to determine group membership. Before Mac OS X v10.4, group membership was based only on a combination of the user's short name and GID.

You can now have groups composed of users with all versions of Mac OS X. When you use Workgroup Manager on Mac OS X Server v10.6 to add a member to a group, you add both the user's short name and GUID, which ensures backward compatibility.

Where Group Accounts Are Stored

Group accounts can be stored in any Open Directory domain. A directory domain can reside on a Mac OS X computer (for example, an Open Directory domain) or it can reside on a non-Apple server (for example, an LDAP or Active Directory server). Workgroup Manager can work with accounts stored in any of these directory domains.

Group accounts must be stored in a directory domain accessible from the server that needs them:

- For services provided by a Mac OS X Server PDC or Windows domain member server, group accounts can be stored in the PDC LDAP directory.
- For services provided by an Active Directory domain member, group accounts can be stored in the Active Directory domain.
- For services provided by a Windows standalone server, group accounts can be stored in the server's local directory domain.
- If a server is configured to access multiple directory domains, group accounts can be stored in any of them.

For more information about the different kinds of Open Directory domains, see *Open Directory Administration*.

Predefined Group Accounts

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

Predefined group name	Group ID	Use
admin	80	A group that users with administrator privileges belong to.
bin	7	A group that owns all binary files.
daemon	1	A group used by system services.
dialer	68	A group for controlling access to modems on a server.
kmem	2	A legacy group used to control access to reading kernel memory.
mail	6	A group historically used for access to local UNIX mail.
_mysql	74	A group that the MySQL database server uses for its processes that handle requests.
network	69	A group that has no specific meaning.
nobody	-2	A group used by system services.

Predefined group name	Group ID	Use
nogroup	-1	A group used by system services.
operator	5	A group that has no specific meaning.
smmsp	25	A group used by sendmail.
sshd	75	A group used for the sshd child processes that process network data.
staff	20	A default group that UNIX users are traditionally placed.
sys	3	A group that 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	A group used when the system doesn't know about the hard drive.
utmp	45	A group that controls who can update the system's list of logged-in users.
_uucp	66	A group used to control access to UUCP spool files.
wheel	0	A group (in addition to the admin group) that users with administrator privileges belong to. Membership is required for using the `su` command.
_www	70	A nonprivileged group that Apache uses for its processes that handle requests.

Administering Group Accounts

Workgroup Manager lets you administer group accounts stored in multiple directory domains.

Creating Group Accounts

To create a group account in a directory domain, you must have directory administrator privileges.

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

To create a group account:

1. In Workgroup Manager, click Accounts.
2. Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.

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

   You can also use a preset or an import file to create a group. For details, see "Creating a Preset for Group Accounts" on page 97 and the appendix, "Importing and Exporting Account Information" on page 272.

From the command line:

1. Identify an unused group ID by entering the following command to display a list of assigned group IDs.

```
$ dscl /LDAPv3/ipaddress -list /Groups PrimaryGroupID | awk '{print $2}'
     | sort -n
```

   Replace *ipaddress* with the location of your directory domain (the way it appears in the search path in Directory Access).

   After you enter the command, the `dscl` tool displays a list of assigned IDs similar to the following output:

```
-2
0
1
25
78
79
501
```

   Important: In this example, select an ID that isn't on the list and that is greater than 501.

2. Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

```
$ dscl localhost
>
```

3. Change the current folder to /LDAPv3/*ipaddress*/Groups by entering the path at the prompt:

```
> cd /LDAPv3/ipaddress/Groups
```

Replace *ipaddress* with the IP address of your directory server.

4. Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

5. Create a group, replacing *officegroup* with the new group account's short name, and specify the group ID, replacing *600* with the primary group ID.

```
> create officegroup PrimaryGroupID 600
```

6. Review the settings of your group by entering the following command, replacing *officegroup* with the group account's short name.

```
> read officegroup
```

7. View the settings for your group account.

Settings for your group account appear similar to the following output:

```
dsAttrTypeNative:apple-generateduid:4B3A5678-E9C1-2EC3-4567-891D234E5678
dsAttrTypeNative:cn: officegroup
dsAttrTypeNative:gidNumber: 600
dsAttrTypeNative:objectClass: posixGroup apple-group extensibleObject top
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:4B3A5678-E9C1-2EC3-4567-891D234E5678
PasswordPlus:********
PrimaryGroupID: 600
RecordName: officegroup
RecordType: dsRecTypeStandard:Groups
```

8. Quit the `dscl` tool.

```
> quit
```

Creating a Preset for Group Accounts

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

Presets are stored in the directory domain that you're viewing. If you change directory domains, the presets you created in the other directory domain are not available.

For instructions on renaming, editing, or deleting group presets, see "Renaming Presets" on page 64, "Editing Presets" on page 64, and "Deleting a Preset" on page 65.

To create a preset for group accounts:

1. In Workgroup Manager, click Accounts.
2. Make sure the server is configured to access the Mac OS X directory domain or non-Apple LDAPv3 domain where the preset is used to create accounts.
3. To create a preset using data in an existing group account, open the account; to create a preset from scratch, create a group account.
4. Fill in the fields with values you want new groups to inherit and delete values you don't want to specify in advance.
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. From the Presets pop-up menu, choose Save Preset, enter a name for the preset, and then click OK.

Editing Group Account Information

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

To make changes to a group account:

1. In Workgroup Manager, click Accounts.
2. Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.

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

   For details, see "Working with Basic Settings for Groups" on page 103, "Working with Member Settings for Groups" on page 106, and "Working with Group Folder Settings" on page 110.

To display group information from the command line:

```
$ dseditgroup officegroup
```

Creating Hierarchical Groups

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

For computers with Mac OS X v10.5 or later, hierarchical groups inherit managed preferences. Members of a hierarchical group have combined preferences managed by their chosen workgroup and by parent groups. They can also inherit preferences from parent groups.

For computers with Mac OS X v10.4 or later, the access permissions of a parent group are inherited. For example, if you set a parent group's ACL permissions so the parent group can't write to a folder, the ACL permissions are propagated so that hierarchical groups also can't write to that folder.

Groups created using Mac OS X Server v10.3 and v10.4 must be upgraded to become parent or child hierarchical groups and use hierarchical preference management. If you don't upgrade groups created using Mac OS X Server v10.3, you can't use hierarchical groups. If you don't upgrade groups created using Mac OS X Server v10.4, you can't use hierarchical preference management with those groups. For more information, see "Upgrading Legacy Groups" on page 101.

To create a hierarchical group:

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

   For instructions, see *Open Directory Administration*.
3. Click the globe icon and choose the domain where you want the hierarchical group to reside.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. To create a group, click the Groups button.
6. In the Members pane, click the Add (+) button to open a drawer that lists the users and groups defined in the directory domain you're working with.

   Make sure the group account resides in a directory domain specified in the search policy of computers the user logs in to.

   The drawer lists user and group accounts. Click the Groups button in the drawer to list group accounts.
7. Drag the group from the drawer to the Members list.

   All members of the hierarchical group also become members of the parent group.
8. Click Save.

To create a hierarchical group from the command line:

- Enter this:

```
$ dseditgroup -o edit [-a childgroup] [-t group] [-u username] [-P
     password] [-n /LDAPv3/ipaddress] parentgroup
```

Parameter	Description
childgroup	The name of the child group you are adding to the parent group
username	The short name of a user with LDAP directory service access
password	The user password
ipaddress	The IP address of your directory server
parentgroup	The name of the parent group that the child group is being added to

To verify a hierarchical group from the command line:

1. Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

```
$ dscl localhost
>
```

2. Change the current folder to /LDAPv3/*ipaddress*/Groups by entering the path at the prompt:

```
> cd /LDAPv3/ipaddress/Groups
```

Replace *ipaddress* with the IP address of your directory server.

3. Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

4. View the members of the group by entering the following (replacing *parentgroup* with the group account's short name):

```
> read parentgroup
```

5. View the setting for your group account.

Settings for the group account appear similar to the following output where the group named parentgroup is shown as nested:

```
dsAttrTypeNative:apple-generateduid:4B3A5678-E9C1-2EC3-4567-891D234E5678
dsAttrTypeNative:apple-group-nestedgroup:1A2B3456-C7D8-9EF1-2345-
     678G912H3456
dsAttrTypeNative:cn: parentgroup
dsAttrTypeNative:gidNumber: 700
dsAttrTypeNative:objectClass: posixGroup apple-group extensibleObject top
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:4B3A5678-E9C1-2EC3-4567-891D234E5678
NestedGroups:1A2B3456-C7D8-9EF1-2345-678G912H3456
PasswordPlus:********
PrimaryGroupID: 700
```

```
RecordName: parentgroup
RecordType: dsRecTypeStandard:Groups
```

To unnest a group from the command line:

- Enter this:

```
$ dseditgroup -o edit [-d childgroup] [-t group] [-u username] [-P
     password] [-n /LDAPv3/ipaddress] parentgroup
```

Parameter	Description
childgroup	The name of the child group you are adding to the parent group
group	The type of account you are changing (in this case, group)
username	The short name of a user with LDAP directory service access
password	The user password
ipaddress	The IP address of your directory server
parentgroup	The name of the parent group that the child group is being added to

Upgrading Legacy Groups

When you upgrade from Mac OS X Server v10.3, or when you import groups created using Workgroup Manager v10.3, existing groups can't use hierarchical preference management unless you first convert them. Upgrading from Mac OS X Server v10.2 or importing groups created in Workgroup Manager v10.2 automatically converts groups during import.

Upgrading legacy groups does not negatively affect group members with client computers running previous versions of Mac OS X.

To convert a legacy group to an upgraded group account:

1. In Workgroup Manager, click Accounts.
2. Make sure that the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.

   For instructions, see *Open Directory Administration*.
3. Click the globe icon and choose the domain where the group account resides.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Click the Groups button and select the legacy group you want to upgrade.
6. In the Members pane, click the Upgrade Legacy Group button and then click Save.

Working with Read-Only Groups

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, NIS domains, and BSD configuration files.

To work with read-only groups:

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

   For information about using Directory Utility to configure server connections, see *Open Directory Administration*. For information about the group account elements that need to be mapped, see the appendix, "Importing and Exporting Account Information."
3. Click the globe icon and then choose the directory domain where the group account resides.
4. Use the panes provided to review the group account settings.

Deleting a Group

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

> *WARNING:* You cannot undo this action.

To delete a group using Workgroup Manager:

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

   To select the account, click the globe icon, choose the directory domain where the account resides, click the Groups button, and then select the group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Choose Server > Delete Selected Group or click the Delete icon in the toolbar.

From the command line:

```
$ dseditgroup -o delete -p -n /LDAPv3/ipaddress -u diradmin groupname
```

Replace *ipaddress* with the IP address of the DNS name of the LDAPv3 server, *diradmin* with the name of the directory administrator, and *groupname* with the name of the group you want to delete.

The `-p` option prompts you for your diradmin password, which is more secure than putting the password in the command you are sending.

For more information, see the `dseditgroup` man page.

Working with Basic Settings for Groups

Basic settings for groups include name, ID, picture path, and comments.

Naming a Group

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

- A *long group name* (for example, English Department Students) is used for display purposes and contains no more than 255 bytes.

  Because long group names support various character sets, the number of characters for long group names can range from 255 Roman characters to as few as 63 characters (for character sets in which characters occupy up to 4 bytes).

- A *short group name* contains as many as 255 Roman characters. Use only the following characters in a short group name:
  - a through z
  - A through Z
  - 0 through 9
  - _ (underscore)
  - - (hyphen)
  - . (period)

  The short name (typically eight or fewer characters) is used by Mac OS X to find group members' user IDs when determining whether a user can access a file as a result of his or her group membership.

  For more information about group membership, see "How Group Accounts Track Membership" on page 93.

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

To work with group names using Workgroup Manager:

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

   To select an account, click the globe icon, choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.

4 Click Basic, then in the Name field (or the Short Name field) review or edit the names and then click Save.

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 the group. The maximum value is 2,147,483,647.

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

To work with a group ID using Workgroup Manager:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to work with.

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

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

4 Click Basic, then in the Group ID field review or edit the ID and click Save.

Before saving a group ID, Workgroup Manager verifies that it is unique in the directory domain you're using.

Choosing a Group's Login Picture

You can quickly change a group's login picture in Workgroup Manager. This picture represents the group in the workgroup chooser of the login window.

Although you can use an image file of any size, you should use an image that is 64x64 pixels in size. If you use a larger image, it is centered and resized to 64x64.

Group pictures are stored as a path to an image file, not as the file itself. This path must be accessible by the computers used by the group. For example, if you enter a path to an image file on the desktop, the image file must be located on the desktop of all computers used by the group. To avoid copying image files to all computers, store image files on a server.

To choose a group's login picture:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to work with.

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

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

4 In the Basic pane, drag a picture to the picture area in the top right.

When you drag a picture to the picture area, the Picture Path field is updated with the new location of the picture. You can also change the picture by editing this path.

5 Click Save.

Enabling a Group's Web Services When Connecting to Mac OS X Server v10.5

Mac OS X Server v10.5 allows groups to easily create a collaborative website. This website uses calendar, wiki, and blog technology to streamline group communication. You can also set up a mailing list so that mail sent to the list is sent to all group members and are archived on the group website.

In Mac OS X Server v10.6, users can set up wikis and blogs while viewing the website. Because of this, Workgroup Manager supports creation of wikis and blogs when you connect to Mac OS X Server v10.5, but not when you connect to Mac OS X Server v10.6.

You can only enable the web calendar and mailing list archive if you first enable the wiki and blog service.

You can choose who views or edits the website:

- "Group members only" includes all members of the group
- "Some group members" (only available for editing) includes group members who are given editing privileges
- "Authenticated users" includes anyone who can authenticate with your organization's directory
- "Anyone" allows everyone, without requiring authentication

You can provide different levels of website access to different subsets of users. For example, you can set up an intranet site where everyone in your organization can view the site (allow "Entire directory" to view services), but only group members can edit it (allow "Group members" to edit services).

When setting up levels of website access, the users who can edit the website are a subset of the users who can view it. For example, you can't let anyone edit the site and allow only group members to view it.

When you create a group, the URL of the group website and the mailing list email address is based on the short name of the group (*shortname@hostname*.com). If you change the group's name after creating it, the URL and mailing list email address do not change.

The administrator computer's search policy must include the server that hosts web services.

To enable a group's web services:

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

   To select an account, click the globe icon, choose the directory domain where the account resides, click the Groups button, and select the group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Choose a server from the "Enable the following services for this group on" pop-up menu.
5. Select the services you want to enable.

   You can only select services that are not disabled by your web server.
6. Choose who can view the group website by using the "can view these services" pop-up menu.

   This option applies to viewing the wiki, blog, calendar, and mailing list archive.
7. Choose who can edit the group website by using the "can write to these services" pop-up menu.

   This option applies to editing the wiki, blog, and calendar.
8. Click Save.

Working with Member Settings for Groups

In Workgroup Manager, use the Members pane for a group to view, add, or remove group members.

When a user name in the Members list appears in italics, the group is the user's primary group.

Adding Users or Groups to a Group

When you want multiple users or groups to have the same file permissions, or when you want to apply the same management settings to all users or groups, add the users or groups to a group.

After assigning a user to a primary group, you don't need to add the user to that group. However, you must specifically add users to other groups.

You can use Workgroup Manager to add a user to a group if the user and group accounts are in an Open Directory domain or the local directory domain. Although some group information doesn't apply to Windows users, you can also add Windows users to groups you create.

Mac OS X Server v10.5 and later supports *hierarchical groups*—groups composed of nested groups. By managing preferences for a parent group, child groups also receive these managed preferences. For more information, see "Understanding Hierarchical Preference Management" on page 169.

To add a user to a group using Workgroup Manager:

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

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

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

From the command line:

1. Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

   ```
   $ dscl localhost
   >
   ```
2. Change the current folder to /LDAPv3/*ipaddress*/Groups by entering the path at the prompt:

   ```
   > cd /LDAPv3/ipaddress/Groups
   ```

   Replace *`ipaddress`* with the IP address of your directory server.
3. Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

   ```
   > auth adminusername
   ```

4 Add the user to the group by entering the following command, replacing *groupPath* with the group's path relative to the current folder, and *userName* with the user's short name:

```
> append groupPath GroupMembership userName
```

For example, if the group's folder is in the /Groups folder, replace *groupPath* with the group's short name. However, if the group's folder is in the /Groups/building1/ folder, replace *groupPath* with building1/*shortName*, where *shortName* is the group's short name.

5 Review the settings of the group by entering the following command, replacing *groupShortName* with the group account's short name:

```
> read groupShortName
```

6 View the settings for the group account.

Settings for the group account appear similar to the following output:

```
dsAttrTypeNative:apple-generateduid:4B3A5678-E9C1-2EC3-4567-891D234E5678
dsAttrTypeNative:cn: officegroup
dsAttrTypeNative:gidNumber: 600
dsAttrTypeNative:memberUid: mchen ajohnson bmiller
dsAttrTypeNative:objectClass: posixGroup apple-group extensibleObject top
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:4B3A5678-E9C1-2EC3-4567-891D234E5678
GroupMembership: mchen ajohnson bmiller
Member: mchen ajohnson bmiller
PasswordPlus:********
PrimaryGroupID: 600
RecordName: officegroup
RecordType: dsRecTypeStandard:Groups
```

7 Quit `dscl` by entering:

```
> quit
```

Removing Group Members

You can use Workgroup Manager to remove group members if the group account and its members reside in an Open Directory domain or the local directory domain.

You can't remove a user's primary group.

To remove group members:

1 In Workgroup Manager, click Accounts.

2 Select the group account you want to work with.

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

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

4 In the Members pane, select the members you want to remove from the group, click the Remove (–) button, and then click Save.

From the command line:

1 Start the `dscl` tool in interactive mode, specifying the computer you are using as the source of directory service data:

```
$ dscl localhost
>
```

2 Change the current folder to /LDAPv3/*ipaddress*/Groups by entering the path at the prompt:

```
> cd /LDAPv3/ipaddress/Groups
```

Replace *ipaddress* with the IP address of your directory server.

3 Authenticate as an administrator by entering the following command, replacing *adminusername* with your administrator user name, and entering your administrator password when prompted:

```
> auth adminusername
```

4 View the current members of the group by entering the following (replacing *officegroup* with the group account's short name):

```
> read officegroup
```

5 View the settings for the group account.

Settings for the group account appear similar to the following output, where the group named `officegroup` has users `mchen`, `ajohnson`, and `bmiller` as members:

```
dsAttrTypeNative:apple-generateduid:4B3A5678-E9C1-2EC3-4567-891D234E5678
dsAttrTypeNative:cn: officegroup
dsAttrTypeNative:gidNumber: 600
dsAttrTypeNative:MemberUid: mchen ajohnson bmiller
dsAttrTypeNative:objectClass: posixGroup apple-group extensibleObject top
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:4B3A5678-E9C1-2EC3-4567-891D234E5678
GroupMembers:2B3A4567-E8C9-9EC2-3456-789D123E4567 1B2A3456-E7C8-9EC1-
     2345-678D912E3456 8B9A1234-E5C6-7EC8-9123-456D78E9123
GroupMembership: mchen ajohnson bmiller
Member: mchen ajohnson bmiller
PasswordPlus:********
PrimaryGroupID: 600
RecordName: officegroup
RecordType: dsRecTypeStandard:Groups
```

6 Remove the user by entering the following command, replacing *ajohnson* with the short name of the user account, *ajguid* with ajohnson's GUID, and *officegroup* with the short name of the group account:

```
> delete officegroup GroupMembership ajohnson
> delete officegroup GroupMembership ajguid
```

7 Review the new settings of the group:

```
> read officegroup
```

8 View the settings for the group account.

Settings for the group account show that the user you removed is no longer a group member, similar to the following output:

```
dsAttrTypeNative:apple-generateduid:4B3A5678-E9C1-2EC3-4567-891D234E5678
dsAttrTypeNative:cn: officegroup
dsAttrTypeNative:gidNumber: 600
dsAttrTypeNative:MemberUid: mchen bmiller
dsAttrTypeNative:objectClass: posixGroup apple-group extensibleObject top
AppleMetaNodeLocation: /LDAPv3/ipaddress
GeneratedUID:4B3A5678-E9C1-2EC3-4567-891D234E5678
GroupMembers:2B3A4567-E8C9-9EC2-3456-789D123E4567 8B9A1234-E5C6-7EC8-
     9123-456D78E9123
GroupMembership: mchen bmiller
Member: mchen bmiller
PasswordPlus:********
PrimaryGroupID: 600
RecordName: officegroup
RecordType: dsRecTypeStandard:Groups
```

9 Quit `dscl` by entering:

```
> quit
```

Working with Group Folder Settings

A group folder offers a way to organize and distribute documents and applications to group members, and gives group members a way to share files with each other.

Group folders are not directly linked to workgroup management, but access and workflow management can be improved by combining the use of group folders with managed preferences for workgroups.

For example, to set a multimedia lab computer specifically for a movie-editing class, you could set Dock preferences for the movie-editing workgroup to display only iMovie and the group folder. Because the group folder is in the Dock, it provides an easily accessible location for students to store and retrieve files.

Group folders aren't mounted on Windows workstations when group members log in to the Windows domain. If the group folder's share point is shared using SMB, a Windows user can go to My Network Places (or Network Neighborhood) and access the contents of the group folder.

Specifying No Group Folder

You can use Workgroup Manager to change a group account with a group folder to one that has no group folder. By default, a new group has no group folder.

To specify no group folder:

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

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

Creating a Group Folder

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

In Workgroup Manager, you can also create group folders that don't reside immediately below a share point. For example, you can organize group folders into several subfolders under a share point that you define.

If Groups is the share point, you can place group folders for students in /Groups/StudentGroups and group folders for teachers in /Groups/TeacherGroups. The full path to a group folder for second-grade students might be /Groups/StudentGroups/SecondGrade.

Group folders are hosted on share points. For instructions about creating share points, see "Setting Up a Share Point" on page 126.

After setting up a group folder, you can automate a group member's access to the group folder when the user logs in by:

- Setting up Dock preferences to make the group folder visible in the Dock. For instructions, see "Providing Easy Access to Group Folders" on page 186.
- Setting up login preferences so that users can click Computer in the Finder to see the group folder share point and the group folders in it. For instructions, see "Providing Easy Access to the Group Share Point" on page 212.

When setting up these preferences, make sure the group is defined in a shared domain in the search policy of the group member's computer. For instructions on setting a computer's search policy, see *Open Directory Administration*.

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

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

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

   To select an account, connect to the server where the account resides, click the globe icon, choose the directory domain where the group account is stored, click the Groups button, and then select the group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Group Folder.
5. To add a 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, to identify an AFP share point named "SchoolGroups" on a server whose DNS name is "myserver.example.com," enter afp://myserver.example.com/SchoolGroups.

   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 at 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 with a network mount record does not cause the group folder to mount when a group member logs in. You can provide easy access to a group folder by managing Dock or login preferences for the group.
6. In the Owner Name fields, enter the short name and long name of the user you want to assign as the owner of the group folder so the user can act as group folder administrator.

To choose an owner from a list of users in the current directory domain, click the Browse (...) button. Click the globe icon in the drawer to choose a different directory domain.

The group folder owner is given read/write access to the group folder.

7 Click Save.

8 To create the folder, use the `ssh` tool to connect to the server hosting the share point and then enter the `CreateGroupFolder` command in Terminal.

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

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

From the command line:

```
$ sudo /usr/bin/CreateGroupFolder
```

For more information, see the `CreateGroupFolder` man page.

Designating a Group Folder for Use by Multiple Groups

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

Usually, a single group has read/write permissions for a group folder. To allow multiple groups to access the same group folder, use Server Admin to add an ACE for every group to the group folder's ACL.

For more information about using Server Admin to apply ACL permissions to folders, see *File Server Administration*.

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

1 In Workgroup Manager, click Accounts.

2 Select the first group account that will use the folder.

To select an account, connect to the server where the account resides, click the globe icon, choose the directory domain where the group account is stored, click the Groups button, and then select the group.

3 Click Group Folder, select the folder you want the group to use, and then click Save.

4 In Server Admin, add an ACE entry that gives the group read/write permissions for the group folder.

5 Repeat this process for each group that you want to use the same group folder.

Setting Up Computers and Computer Groups

6

Use this chapter to set up and manage individual computers and groups of computers.

To manage an individual computer, you must create a computer account. To manage a group of computers, you must create a computer group composed of computer accounts or of other computer groups.

Use Workgroup Manager to view, create, edit, and delete computers and computer groups.

To view computers in Workgroup Manager, click the Computers button above the accounts list. To view computer groups in Workgroup Manager, click the Computer Groups button above the accounts list.

About Computer Accounts

A computer account stores data that allows Mac OS X Server to identify and manage individual computers. To create computer groups, you must first create computer accounts for each individual computer.

Before setting up a computer, you need the computer's name and address. You usually use the computer name specified in a computer's Sharing preferences, or you can use a descriptive name that you find more suitable.

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

For Windows computers, you must know the NetBIOS name of each Windows client computer. This name is entered in the name field. You don't need to know the Ethernet address of Windows client computers.

When a computer starts up, Mac OS X tries to match the computer's Ethernet address with a computer account. If a matching computer account is found, the computer uses the managed preferences for that computer account and the computer groups it belongs to. If no matching computer account is found, the computer uses the managed preferences for the Guest Computer account.

Creating Computer Accounts

To create a computer account in a directory domain, you must have administrator privileges.

When you enter the Ethernet ID, it must be entered correctly so the DHCP server can find the computer. It must follow these rules:

- It must be entered using hexadecimal numbers. Hexadecimal numbers include digits 0–9 and letters a–f.
- Bytes must be separated by colons. Bytes are comprised of two hexadecimal numbers.
- All bytes with a single hexadecimal number should have a leading zero. For example, the following Ethernet ID is invalid because the single hexadecimal numbers do not have leading zeros:

  7:8:9:a:b:c

  However, the following Ethernet ID is valid because the hexadecimal numbers have leading zeros:

  07:08:09:0a:0b:0c
- The letters a–f must be entered in lower case.

To create a computer account:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the directory domain where you want to store the computer account.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click the Computers button.
5. Choose Server > New Computer (or click New Computer in the toolbar) and then enter long and short names for the computer.
6. Click General.
7. To add a comment, in the Comment field, enter a comment.

   Comments and keywords make it easier to search for the computer.
8. To associate keywords with the computer, click the Add (+) button next to the keywords list.

If keywords that you want to associate aren't listed in the master keyword list, click Edit Keywords, click the Add (+) button, enter a name for the keyword, and click OK.

Select the keywords you want to associate with the computer and click OK.

9 Enter the hardware UUID in the Hardware UUID field.

To find the hardware UUID:

- On client computers with Mac OS X v10.6 or later, open System Profiler (located in /Utilities), view Hardware, and review the Hardware UUID entry.
- On client computers with Mac OS X v10.5.7 or later, open System Profiler and choose File > Save. After saving the System Profiler log file, enter the following in Terminal:

  ```
  grep IOPlatformUUID  system_profiler_log.spx
  ```

  Replace *system_profiler_log* with the path and name of the System Profiler log file. If your client computer is running Mac OS X v10.5.6 or earlier, update it to Mac OS X v10.5.7 or later.

If your client computers run Mac OS X v10.4, don't enter a hardware UUID.

10 Click Network and enter the Ethernet ID for the computer and its IP address (if the computer receives a static IP).

11 Click Save.

Working with Guest Computers

If a computer connects to your directory domain, and the computer doesn't have any managed settings in its record or computer groups that its record is in, that computer is treated as a guest computer. If there is no computer record, the computer is treated as a guest computer. Settings for the guest computer account apply to these unknown computers.

To apply specific management settings to a computer, don't use the guest computer account to manage it. Create a computer account for it.

Note: You can't change the name of a guest computer. Because the Guest Computer account is associated with all unknown computers, you can't enter network settings to identify the computer.

To set up the guest computer account:

1 In Workgroup Manager, click Accounts.

2 Click the globe icon and choose the directory domain that contains the guest computer account.

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

4 Click the Computers button (on the left).

5 Choose Server > Create Guest Computer.

6 Select the Guest Computer account.

7 Click General, enter a comment or add keywords, and then click Save.

Working with Windows Computers

Every Windows computer that joins the Windows domain of a Mac OS X Server primary doman controller (PDC) must have a computer account, which identifies the Windows computer by its NetBIOS name.

The computer account for a Windows computer also contains information for authenticating the computer as a trusted workstation in the Windows domain. Mac OS X Server creates this information in the form of a UID and a GID.

You can add Windows computer accounts to computer groups, but Windows computers don't receive managed preferences.

Important: Don't create computer accounts for Windows 2000 or Windows XP computers. If you do, they might not be usable for domain login. Instead, use the Windows software on these computers to join them to the Windows domain. For information, see *Open Directory Administration*.

About Computer Groups

A computer group comprises computers with the same preference settings. You can use Workgroup Manager create and modify computer groups.

To edit computer groups or computer group preferences, you must have directory administrator privileges. For instructions on assigning administrator privileges for a directory domain, see "Giving a User Full Administrative Capabilities" on page 75.

Differences Between Computer Groups and Computer Lists

Before Mac OS X Server v10.5, *computer lists* were used to manage computers. Computer lists and computer groups function similarly. By managing a computer list or a computer group, you are managing all individual computers within them.

There are two major differences between computer groups and computer lists:

- Computer groups allow you to include other computer groups. You can then manage hierarchical groups by managing the parent computer group.
- A computer can be a member of multiple computer groups. However, a computer can only be a member of a single computer list.

Ideally, all members of a computer group are either computers running Mac OS X v10.5 or later, or other computer groups. Computer groups that include computers running Mac OS X v10.4 or earlier act like any other computer group of computers running Mac OS X v10.5 or later—that is, computers can belong to multiple computer groups, and you can form hierarchical groups.

The computer group acts like a computer list for computers running earlier versions of Mac OS X. Computers can only belong to one list, and nesting the computer group has no effect on the computer.

Administering Computer Groups

You can use Workgroup Manager to administer computer groups stored in various directory domains.

Creating a Computer Group

When you create a computer group, keep in mind the following:

- A computer group is a group of computers that have the same preference settings and are available to the same users and groups.
- You can add up to 2000 computers to a computer group.

You can create hierarchical groups to manage computers with Mac OS X v10.5 or later. Hierarchical groups inherit managed preferences. Computers in a hierarchical group have combined preferences managed by their computer group and by parent computer groups. They can also inherit preferences from parent computer groups.

To set up a computer group:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the directory domain where you want to store the computer group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click the Computer Groups button (on the left).
5. To use a preset, choose one from the Presets pop-up menu.
6. Choose Server > New Computer Group (or click New Computer Group in the toolbar), and then enter a name for the computer group.
7. Click Basic.
8. Optionally, add a comment.

   Comments are useful for providing information about a computer's location, configuration (for example, a computer set up for individuals with special needs), or attached peripherals. You could also use the comment for identification information, such as the computer's model or serial number.
9. Click Members, click the Add (+) button, and then drag computers or computer groups listed in the drawer to add them to the computer group.

   You can also click the Browse (...) button, select a computer, and click Add.
10. Click Save.

After setting up a computer group, you can manage preferences for it. For more information about using managed preferences, see "Customizing the User Experience" on page 158, and Chapter 10, "Managing Preferences."

Creating a Preset for Computer Groups

You can select settings for a computer group and save them as a preset. Presets work like templates, allowing you to apply preselected settings and information to new computer groups.

Using presets, you can easily set up multiple computer groups that use similar settings. However, you can only use presets when creating a computer group. You can't use a preset to change a computer group.

To set up a preset for computer groups:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the directory domain where you want to create a computer group using presets.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click the Computer Groups button (on the left).
5. Create a computer group by clicking New Computer Group or by selecting an existing computer group (on the left).
6. Fill in the information in the Basic and Members panes.
7. From the Presets pop-up menu, choose Save Preset.

After creating a preset, you can change its settings, change its name, or delete it:

To do this	Do this
Change the preset's settings	Create a computer group based on the preset and change the computer group settings. Save the preset using the same name as the old preset. When you change a preset, existing accounts that were created with it are not updated to reflect the changes.
Change the name of a preset	Choose Rename Preset from the Presets pop-up menu, choose the preset, enter a new name, and then click OK.
Delete a preset	Choose Delete Preset from the Presets pop-up menu, select the preset, and then click Delete.

Using a Computer Group Preset

When you create a computer group, you can choose any preset from the Presets pop-up menu to apply initial settings. You can further modify computer group settings before you save the list.

When you save the computer group, you can't use the Preset menu again for that list (for example, you can't apply a different preset to the group).

To use a preset for computer groups:

1. In Workgroup Manager, click Accounts.
2. Click the globe icon and choose the directory domain where you want to store the computer group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click the Computer Groups button (on the left) and then click Basic.
5. From the Presets pop-up menu, choose a preset.
6. Choose Server > New Computer Group (or click New Computer Group in the toolbar).
7. Add or update settings as needed and then click Save.

Adding Computers or Computer Groups to a Computer Group

You can easily add computers and computer groups to an existing computer group using Workgroup Manager.

Hierarchical computer groups are supported in Mac OS X Server v10.5 or later. If you add computer groups containing client computers running Mac OS X v10.4 or earlier, those clients don't receive managed preferences from parent computer groups.

To add computers or computer groups to a computer group:

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

   To select the computer group, click the globe icon, choose the directory domain that contains the computer group, click the Computer Groups button, and then select the computer group.
3. To authenticate, click the lock and enter the name and password of a directory administrator.
4. Click Members, click the Add (+) button, and then drag computers or computer groups from the drawer to the list.

   You can also click the Browse (...) button, select a computer, and then click Add.

   Continue adding computers and computer groups until the list is complete.
5. Click Save.

Removing Computers and Computer Groups from a Computer Group

If you remove a computer from a computer group, you can still manage it by managing its computer account or by adding it to another computer group.

To remove a computer or computer groups from a computer group:

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

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

Deleting a Computer Group

If you no longer need a computer group, you can use Workgroup Manager to delete it.

> *WARNING:* You cannot undo this action.

To delete a computer group:

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

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

Upgrading Computer Lists to Computer Groups

Computer lists are groups of computers created in Mac OS X Server v10.4 or earlier. Computer lists can only include computers, not other computer lists. Computer groups can include computers and hierarchical computer groups. You can hierarchically manage preferences for computer groups.

Computer groups can include computers running earlier versions of Mac OS X. These computers don't receive hierarchical preference management.

To upgrade computer lists to computer groups:

1. In Workgroup Manager, click Accounts, click the Computer Groups button, and then select a computer list.
2. In the Basic pane, click Upgrade Computer List to Group.

Setting Up Home Folders

7

Use this chapter to set up and manage home folders.

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

To set up share points that host home folders, you can use Server Admin. After setting up share points, you can then use Workgroup Manager to set up home folders on the share points.

About Home Folders

You can set up Mac OS X home folders so they can be accessed by Apple Filing Protocol (AFP) or Network File System (NFS).

To set up a home folder for a user in Workgroup Manager, use the Home pane when viewing a user's account.

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

A user's home folder doesn't need to be stored on the same server as the directory domain containing the user's account. In fact, distributing directory domains and home folders across servers can help balance the workload. For more information, see "Distributing Home Folders Across Multiple Servers" on page 125.

The home folder you designate in the Home pane can be used when logging in from a Windows workstation or a Mac OS X computer. This can be helpful for a user whose account resides on a server that is a Windows primary domain controller (PDC).

WARNING: If the absolute path from the client to the network home folder on the server contains spaces or more than 89 characters, some types of clients won't connect. For example, a client using automount with an LDAP-based AFP home folder might not be able to access its home folder. The "/" character is considered a character.

There are additional limitations on the maximum path length, depending on the version of Mac OS X used by clients. For more information, see the Apple Service & Support website article, "Avoid spaces and long names in network home directory name, path," at support.apple.com/kb/HT2799.

Hosting Home Folders for Mac OS X Clients

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

The preferred protocol is AFP because it provides authentication-level access security. A user must log in with a valid name and password to access files.

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

Hosting Home Folders for Other Clients

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

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

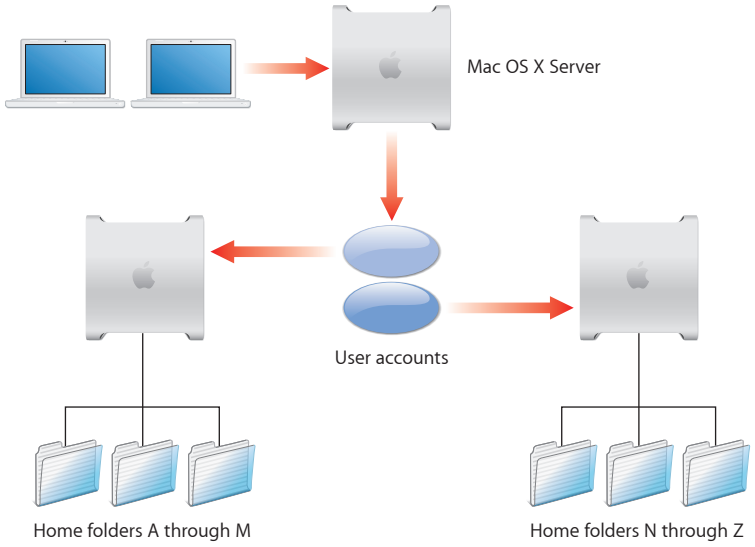
In addition to having home folders, Windows users also have roaming profiles. With roaming profiles, each user has the same profile when he or she logs in to the domain from any Windows workstation on the network.

A roaming profile stores a Windows user's preference settings (screensaver, colors, backgrounds, event sounds, and so on), favorites, My Documents folder, and more, in a share point on a Mac OS X Server. By default, a user's roaming profile is stored in a predetermined folder on the PDC, and backup domain controllers (BDCs) have an up-to-date copy of this folder.

The default share point for Windows home folders is the same as the share point for Mac OS X home folders. The default share point for user profiles is the /Users/Profiles/ folder on the PDC and BDC servers. (This SMB share point is not shown in Workgroup Manager.) You can set up alternate SMB share points for home folders and user profiles on the PDC server or on domain member servers.

Distributing Home Folders Across Multiple Servers

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



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

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

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

Step 2: Set up an automountable share point for home folders on each home folder server For information about how to set up automountable share points, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 127.

Step 3: Create the user accounts in the shared domain on the accounts server For information about specifying which share point is used for a user's home folder, see "Administering Home Folders" on page 131.

Step 4: Set up the directory services of the client computers so their search policy includes the shared directory domain on the accounts server For information about configuring search policies, see *Open Directory Administration*.

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

Administering Share Points

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

Setting Up a Share Point

You can use Server Admin to set up share points and then use the share points to host local home folders. Or you can mount the share point so it hosts network home folders.

To set up a share point:

1. Open Server Admin and connect to the server where you want to host the share point.

   To connect to the server, choose Server > Connect, enter the server address in the Address field, and then authenticate as a server administrator.

   If you're already connected, you'll see Disconnect (instead of Connect) in the Server menu.

2. Select the server and click File Sharing.
3. Click Volumes, then display folders within volumes by clicking Browse.
4. Select the volume or folder that will become a share point.

   To create a folder, select a parent folder or volume and click New Folder, enter the name of the folder, and click Create.

5. In Permissions, select entries in the list, click the Edit (pencil) button to change their name or permissions, and change the settings as follows:

UNIX Class	Name	Permission
Owner (single silhouette)	admin	Read and Write
Group (several silhouettes)	admin	Read
Others (globe)	Others	Read

6. Click Share and then click Save.

Setting Up an Automountable AFP Share Point for Home Folders

You can use Server Admin to set up an AFP share point for home folders.

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

Using an automountable share point ensures that the home folder appears in /Network/Servers when the user logs in to a Mac OS X computer configured to access the shared domain.

Users can access home folders on any automountable share point with guest access enabled.

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

1. If you do not have a share point to host home folders, create one.

   For instructions, see "Setting Up a Share Point" on page 126.

2. Open Server Admin and connect to the server that hosts the share point.

   To connect to the server, choose Server > Connect, enter the server address in the Address field, and authenticate as a server administrator.

   If you're already connected, you'll see Disconnect (instead of Connect) in the Server menu.

3. To view a list of available services, use the disclosure triangle next to your server.

   If Server Admin doesn't list the AFP service, click the Add (+) button, choose Add Service, select AFP, and then click Save.

4. Select the AFP service and click Settings.

5. In Access, select "Enable Guest access" and click Save; then if AFP is not running, click Start AFP.

   For more information about administering AFP service, see *File Server Administration*.

6. Select the server and click File Sharing.

7. Click Share Points and then select the share point.

8. In Share Point, select Enable Automount.

   A configuration dialog appears. If not, click Edit and continue.

9. Choose your directory domain from the Directory pop-up menu, choose AFP from the Protocol pop-up menu, select "Use for User home folders," and click OK.

10. In the dialog that appears, authenticate as the directory administrator and then click OK.

11. Click Protocol Options.

12 In AFP, select "Share this item using AFP" and "Allow AFP guest access."

When you enable guest access, it is enabled for all home folders in the share point.

By default, guests can only access /Public and /Sites folders in home folders. When a guest browses the home folder server, they can see who has home folders on that server but they are restricted to opening guest-access-enabled folders.

Guests can also use *~user-short-name/*Public to access a user's Public folder.

13 To prevent SMB access to the share point, in SMB, deselect "Share this item using SMB."

14 To prevent FTP access to the share point, in FTP, deselect "Share this item using FTP."

15 To prevent NFS access to the share point, in NFS, deselect "Export this item and its contents to."

16 Click OK to close the Protocol Options dialog and then click Save.

From the command line:
You can also set up a share point using the `sharing` command in Terminal. For more information, see its man page.

Setting Up an Automountable NFS Share Point for Home Folders

Although AFP is the preferred protocol for accessing home folders (because of the security it offers), you can use Server Admin to set up a network NFS share point for home folders.

NFS share points can be used for home folders of users defined in shared directory domains, such as an Open Directory domain or an Active Directory domain.

The NFS share point must be automountable—that is, it must have a network mount record in the directory domain where the user account resides.

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

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

1 If you do not have a share point to host home folders, create one.

For instructions, see "Setting Up a Share Point" on page 126.

2 Open Server Admin and connect to the server that hosts the share point.

To connect to the server, choose Server > Connect, enter the server address in the Address field, and then authenticate as a server administrator.

If you're already connected, you'll see Disconnect (instead of Connect) in the Server menu.

3 To view a list of available services, use the disclosure triangle next to your server.

If Server Admin doesn't list the NFS service, click the Add (+) button, choose Add Service, select NFS, and then click Save.

4. Select the NFS service, then if NFS is not running, click Start NFS.

   For more information about administering NFS service, see *File Server Administration*.

5. Select the server and click File Sharing.
6. Click Share Points and then select the share point.
7. In Share Point, select Enable Automount and then click Edit.
8. Choose your directory domain from the Directory pop-up menu, choose NFS from the Protocol pop-up menu, select "Use for User home folders," and click OK.
9. In the dialog that appears, authenticate as the directory administrator and then click OK.
10. Click Protocol Options.
11. In NFS, select "Export this item and its contents to" and choose Client List.
12. Add client computers that you want to have access to the share point.

    Click the Add (+) button and enter the IP address or host name of a client you want to add to the computer group.

    Click the Remove (–) button to remove the selected computer from the list.
13. In the Mapping pop-up menu, choose "Root to Nobody."
14. In the Minimum Security pop-up menu, choose the minimum level of authentication security required with the computers.

    If your computers can't authenticate with this level of security, they can't use NFS share points.
15. To prevent AFP access to the share point, in AFP, deselect "Share this item using AFP."
16. To prevent SMB access to the share point, in SMB, deselect "Share this item using SMB."
17. To prevent FTP access to the share point, in FTP, deselect "Share this item using FTP."
18. Click OK to close the Protocol Options dialog and then click Save.

From the command line:
You can also set up a share point using the `sharing` command in Terminal. For more information, see its man page.

Setting Up an SMB Share Point

You can use Server Admin to:

- Enable or disable access to a share point that uses SMB
- Change the share point name that SMB clients see
- Choose whether guest access and opportunistic locking is allowed

- Set the default permissions for new files and folders in the share point

SMB share points can't be used for Mac OS X home folders but they can be used for Windows home folders.

Note: Don't use a slash (/) in the name of a folder or volume you plan to share. Users trying to access the share point might have trouble seeing it.

To create an SMB share point and set permissions:

1. If you do not have a share point to host home folders, create one.

   For instructions, see "Setting Up a Share Point" on page 126.

2. Open Server Admin and connect to the server that hosts the share point.

   To connect to the server, choose Server > Connect, enter the server address in the Address field, and authenticate as a server administrator.

   If you're already connected, you'll see Disconnect (instead of Connect) in the Server menu.

3. To view a list of available services, use the disclosure triangle next to your server.

   If Server Admin doesn't list the SMB service, click the Add (+) button, choose Add Service, select SMB, and then click Save.

4. Select the SMB service.
5. In General, select Standalone Server from the Role pop-up menu.
6. In Access, select "Allow Guest access."
7. Click Save and then click Start SMB.

   If SMB is already running, the Start SMB button is replaced by the Stop SMB button.

8. Select the server and click File Sharing.
9. Select the share point.
10. In Share Point, click Protocol Options.
11. In SMB, select "Share this item using SMB."
12. To allow unregistered users access to the share point, select "Allow SMB guest access."

    For greater security, don't select this item.

13. To change the name that clients see when they browse for and connect to the share point using SMB, enter a new name in the "Custom SMB name" field.

    Changing the custom SMB name doesn't affect the name of the share point itself, only the name that SMB clients see.

14. Select the type of locking for this share point:

    - To allow clients to use opportunistic file locking, select "Enable oplocks."

Important: Do not enable oplocks for a share point that's using a protocol other than SMB.

For more information on oplocks, see *File Server Administration*.

- To set standard locks on server files, select "Enable strict locking."

15 Choose a method for assigning default UNIX access permissions for new files and folders in the share point:

- To set new items to adopt permissions of the enclosing item, select "Inherit permissions from parent."
- To assign specific permissions, select "Assign as follows" and use the Owner, Group, and Everyone pop-up menus.

16 To prevent AFP access to the share point, in AFP, deselect "Share this item using AFP."

17 To prevent NFS access to the share point, in NFS, deselect "Export this item and its contents to."

18 To prevent FTP access to the share point, in FTP, deselect "Share this item using FTP."

19 Click OK to close the Protocol Options dialog and then click Save.

From the command line:
You can also set up a share point using the `sharing` command in Terminal. For more information, see its man page.

Administering Home Folders

You can use Workgroup Manager to assign a home folder location to user accounts. To assign a home folder location, you must create a share point. For instructions on creating share points, see "Setting Up a Share Point" on page 126.

Specifying No Home Folder

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

Important: Portable home directories require that you specify a network home folder.

To define no home folder:

1 In Workgroup Manager, click Accounts.

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

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

3 Click the Users button and select user accounts.

4 Click Home and select (None) from the list.

5 Click Save.

Creating a Home Folder for a Local User

You can use Workgroup Manager to define home folders for users whose accounts are stored in a server's local directory domain.

You might want to use local user accounts on standalone servers (servers not accessible through a network) and for administrator accounts on a server. These accounts are meant to be used by those logging in to the server locally. They are not meant to be used by network users.

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

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

To create a home folder for a local user:

1 If you don't have a share point, create one.

For instructions, see "Setting Up a Share Point" on page 126.

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

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

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

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

5 If the folder you want to use is a share point, select it.

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

6 If the folder isn't a share point, click the Add (+) button; then, in the dialog, enter the path to the folder in the Full Path field (leaving the other two fields blank) and click OK.

For example, to use the local /Users folder, enter:

/Users/*usershortname*

Replace *usershortname* with the short name of the user.

Don't use a terminating slash.

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

8 Click Create Home Now and then click Save.

If you do not click Create Home Now before clicking Save, the home folder is created the next time the user logs in remotely. However, clients can only connect to servers hosting share points in the local domain.

For instructions on setting up a share point for Mac OS X clients, see "Creating a Network Home Folder" on page 133.

From the command line:

- To create a home folder for a user:

```
$ sudo createhomedir -u uid
```

In addition to the *uid,* you can also use the user's short name.

- To create a home folder for users in the local domain:

```
$ sudo createhomedir [(-a|-l|-n domain)] -u uid
```

You can also create a user's home folder using the `serversetup` tool.

- To create a home folder for a user:

```
$ sudo /System/Library/ServerSetup/serversetup -createHomedir uid
```

The command displays a `1` if the user ID you specify doesn't exist.

For more information, see the `createhomedir` man page.

In all cases, home folders are created on the server where you run the tool.

Creating a Network Home Folder

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

A user's network home folder can reside in any AFP or NFS share point that the user's computer can access.

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

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

To create a network home folder for AFP or NFS share points:

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

For instructions, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 127, or "Setting Up an Automountable NFS Share Point for Home Folders" on page 128.

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

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

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

4 Click Home; then in the share points list select the share point you want to use.

The list displays automountable network-visible share points in the search policy of the server you are connected to, as well as custom home folder locations in the directory domain.

If the share point you want to select is not listed, try clicking Refresh. If the share point still does not appear, it might not be automountable.

5 Set up the share point to have a network mount record configured for home folders as described in step 1, or create a custom home folder location as described in "Creating a Custom Location for Home Folders" on page 135.

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

7 Click Create Home Now and then click Save.

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

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

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

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

From the command line:
You can also create a network home folder using the `createhomedir` command in Terminal. For more information, see "Creating a Home Folder for a Local User" on page 132.

Creating a Custom Location for Home Folders

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

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

To create a custom location for home folders, your share point must be configured correctly.

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

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

For instructions, see "Setting Up an Automountable AFP Share Point for Home Folders" on page 127, or "Setting Up an Automountable NFS Share Point for Home Folders" on page 128.

Important: The following procedure requires Mac OS X Server v10.4.3 or later.

To create a custom home folder using Workgroup Manager:

1. Make sure the share point exists and is configured correctly.
2. To have the home folder reside beneath a folder under the share point, use Workgroup Manager or the Finder to create all folders in the path between the share point and where the home folder resides.
3. In Workgroup Manager, click Accounts and then select the user account you want to work with.

   To select an account, connect to the server where the account resides, click the globe icon, choose the directory domain where the user account is stored, click the Users button, and then select the user account.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Click Home.

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

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

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

8 In the Path to Home Folder field, enter the path from the AFP share point to the home folder, including the home folder but excluding the share point.

For an NFS share point, leave this field blank.

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

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

9 In the Full Path field, enter the full path to the home folder, including the home folder itself, in this format:

[/Network/Servers/*servers-host-name/*][Volumes/[*drive/*]*volume/*]*share-point/path*

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

Replace the following elements:

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

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

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

The following is a Home entry for a custom home folder in the Hard-Drive volume stored in a server located at server.example.com:

/Network/Servers/server.example.com/Volumes/Hard-Drive/Homes/Teachers/SecondGrade/Smith

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

/Network/Servers/server.example.com/Volumes/external-HD/HomeFolders/Homes/Teachers/SecondGrade/Smith

10 Click OK.

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

12 Click Create Home Now and then click Save.

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

Note: Home folders are created the first time a user logs in only on share points served through an AFP or SMB server. You must create NFS home folders manually.

Setting Up a Home Folder for a Windows User

Using Workgroup Manager, you can set up a network home folder that mounts when a Windows user logs in to a Windows domain. Normally, the same network home folder is also mounted if the user logs in on a Mac OS X computer. You can also set up separate home folders if you prefer.

You can create a home folder in any existing share point, or you can create the home folder in the /Users folder—a predefined share point.

To create a home folder in a new share point, create the share point first. The share point for a Windows home folder must be on a Windows domain member server or the PDC server and use SMB protocol. For instructions, see "Setting Up an SMB Share Point" on page 129.

If the share point is used for Mac OS X home folders, it must also use AFP or NFS and have a network mount record configured for home folders.

Set the Windows home folder for a user account in the Mac OS X Server PDC LDAP directory. If you have a BDC, the PDC server replicates changes to it.

To set up a home folder in an existing share point:

1 In Workgroup Manager, open the user account where you want to set up a home folder.

To open an account, click Accounts, click the globe icon below the toolbar, and then open the PDC LDAP directory.

To edit home folder information, click the lock to authenticate as an LDAP directory administrator and then select the user in the user list.

2 To use the same network home folder for Windows as for Mac OS X, click Home, specify the share point to use, and then do the following:

- In the share points list, select /Users or the share point you want to use and then click Create Home Now.

  If you want to select /Users but it isn't listed, click the Add (+) button and then in the Full Path field, enter:

  /Users/*usershortname*

  Replace *usershortname* with the first short name of the user account you're configuring.

- Optionally, enter a disk quota for the user's home folder and specify megabytes (MB) or gigabytes (GB).

  Important: This quota also applies to the user's roaming profile if it's on the same volume as the home folder. Make sure the quota is adequate for both folders for an entire work session. A user's profile folder includes the My Documents folder and the Internet Explorer cache, which often use considerable disk space. For more information, see "Setting Disk Quotas for Windows Users to Avoid Data Loss" on page 140.

3 Click Windows and enter the home folder location in the Path field:

- To use the same home folder for Windows login and Mac OS X login, leave Path blank. You can also specify this home folder by entering a UNC path that doesn't include a share point:

  *servername**usershortname*.

  Replace *servername* with the NetBIOS name of the PDC server or a Windows domain member server where the share point is located. You can see the server's NetBIOS name by opening Server Admin and clicking SMB in the Servers list. Then click Settings, click General, and look at the Computer Name field.

  Replace *usershortname* with the first short name of the user account you're configuring.

- To specify a different SMB share point, enter a UNC path that includes the share point:

  *servername**sharename**usershortname*

  Replace *sharename* with the name of the share point.

4 From the Hard Drive pop-up menu, choose a drive letter.

The default drive letter is H. Windows uses the drive letter to identify the mounted home directory.

5 Click Save.

6 If the Path field isn't blank, make sure the specified share point contains a folder for the user's home folder.

The folder's name must match the user's first short name and the user must have read and write permission for the folder.

If the Path field is blank, the home directory share point doesn't need to contain a home folder for the user. In this case, Mac OS X Server creates a home folder in the share point specified in the Home pane.

Setting Disk Quotas

You can limit the disk space users have available to store files in the volume where their home folders reside.

This quota applies to all files that the user stores in the volume where his or her home folder resides, including all files stored in the user's drop box. Therefore, when a user places files in another user's drop box, it can affect the other user's disk quota or have other effects, such as these:

- 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, when you copy a file to another folder, you remain the owner and the copy operation reduces *your* disk quota on that partition.

WARNING: If you set a disk quota on a user with a mobile account, the quota only affects the user's network home folder. There are no quota restrictions on the user's local home folder.

Setting the quota too low can cause sync issues and data loss. For example, if you set a 250 MB quota and the user uses 500 MB on his or her local home folder, the mobile account doesn't sync entirely.

The home folders sync until the 250 MB quota is met, and unsynced files remain local. When the user logs in to another computer and syncs, only 250 MB of data syncs from the network home folder.

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

1 In Workgroup Manager, click Accounts.

2 Select the user account you want to work with.

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

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

4 Click Home, specify the disk quota using the Disk Quota field and the adjacent pop-up menu, and then click Save.

5 Make sure disk quotas are enabled for the volume where the share point resides.

6 In Server Admin, select the server hosting home folders and then click File Sharing.

7 Click Volumes and then select the volume that stores home folders.

8 Click Quotas, select "Enable quotas on this volume," and then click Save.

Setting Disk Quotas for Windows Users to Avoid Data Loss

A disk quota that applies to a Windows user's roaming profile folder must be large enough to cover the user's expected data storage needs for a work session.

A Mac OS X Server PDC enforces quotas on a roaming profile folder only at the end of a work session when the user logs out and the Windows computer copies the local profile to the roaming profile on the server.

If the copied local profile exceeds the quota, the roaming profile won't be updated with changes affecting the local profile since the user logged in.

If enforcing a user's disk quota prevents an update of the user's roaming profile, and the user later logs in using a different Windows computer, Windows could load and apply the outdated roaming user profile from the server.

The server can't enforce the quota incrementally on the roaming profile folder because the Windows computer updates only the local profile during a work session. (The server enforces a quota incrementally on changes to the home folder.)

A roaming profile folder is subject to the same disk quota as the home directory if both are on the same volume. A user's profile directory is not subject to a disk quota if it's on a different volume from the user's home directory or the home directory is not subject to a disk quota.

Because a quota that covers the roaming profile directory also covers the home directory, make sure the quota is adequate for an entire work session and the user's home folder. A user's profile folder includes the My Documents folder and the Internet Explorer cache, which often uses a considerable amount of disk space.

The recommended minimum quotas are:

- 10 MB for a user who logs in only from Windows workstations
- 20 MB for a user who logs in from Windows and Mac OS X computers

Using Presets to Choose Default Home Folders

You can define default home folder settings to use for new users by using a preset to predefine them. For information about defining and using presets, see "Using Presets to Create Accounts" on page 63.

Moving Home Folders

To move a home folder, create a new home folder, copy the contents of the old home folder into the new home folder, and then delete the old home folder.

Deleting Home Folders

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

Managing Portable Computers

8

Use this chapter to learn about tools available to manage portable computers.

Mac OS X Server allows you to create and manage mobile accounts for users of portable computers.

About Mobile Accounts

If your organization uses portable computers, assign mobile accounts to users. This allows you to manage their preferences and control their level of access to local and network resources. These mobile accounts, which are designed for portable computers, provide many advantages over local or network accounts.

A mobile account includes a network home folder and a local home folder. Having these two types of home folders allows users to take advantage of features available for local and network accounts. You can sync specific folders in these two home folders, creating a portable home directory.

Syncing ensures that users access their most recently updated files when they connect to the network. If a user modifies files on different computers, when he or she connects to the network and syncs, his or her computer retrieves the most recently synced file.

Mobile accounts also cache authentication information and managed preferences. A user's authentication information is maintained on the directory server but is cached on the local computer. With cached authentication information, a user can log in using the same user name and password, even if he or she is not connected to the network.

For example, if a student has a mobile account, the student's login name, password, and preferences defined for the user account, workgroups, and computer are the same at school and at home. If you change these items, the local versions are updated when the user logs in at school.

About Portable Home Directories

A portable home directory is a synced subset of a user's local and network home folders. You can configure which folders to sync and how often to sync them. Users can also initiate syncing. By syncing key folders, a user can work on or off the network and experience the same work environment.

Because the user has a local home folder that only syncs periodically or at login and logout, the mobile account reduces network traffic, expediting server connections for users who need to access the server.

The computer locally caches temporary files. This improves network and individual computer performance because the user's computer locally caches files like webpages.

Because GUIDs for the local user account on the user's computer and in the network user account on an Open Directory server are the same, file permissions are the same whether the user logs in using the local user account (while disconnected from the network) or the network user account.

You can assign mobile accounts to users with accounts stored in an Active Directory domain. To manage sync settings for these mobile accounts, extend the Active Directory schema to accept and map Open Directory attributes.

There are two ways to create mobile accounts:

- Use Workgroup Manager to enable syncing of user accounts
- Allow network users to create mobile accounts themselves

For instructions on using Workgroup Manager to enable syncing, see "Creating a Mobile Account" on page 215.

Users with network accounts who have administrative access to their computers can create mobile accounts, which also creates a portable home directory. You can manage their sync settings in the Rules panes of Mobility preferences.

To prevent users from creating mobile accounts, you can choose not to show Accounts in their System Preferences. For instructions on denying access to specific System Preferences, see "Managing Access to System Preferences" on page 239.

You can also manage Mobility preferences so users they can't create mobile accounts. For instructions on managing Mobility preferences, see "Preventing the Creation of a Mobile Account" on page 216.

Logging In to Mobile Accounts

If a user has created a portable home directory, logging in to a mobile account is similar to logging in to a local account. The user selects his or her account and then enters the correct password to complete the login. If the account is not displayed, the user must enter a login name and password. If you enabled login and logout syncing, the user's folders sync and the user's desktop appears.

If the user does not have a mobile account with a portable home directory, different steps are required after authentication. One of the following occurs, depending on mobile account creation settings:

- If you deselected "Require confirmation before creating mobile account," the computer creates the mobile account.
- If you selected "Require confirmation before creating mobile account," the user sees a confirmation dialog that allows him or her to create a portable home directory, delay it, or not create a portable home directory and disable the dialog until the user holds down the Option key during login.

You can allow the user to choose which volume stores the user's local home folder in Mobility options. Before the mobile account is created, the user must choose where to store the local home folder.

Mobile accounts remain on the computer even when the user logs out or disconnects from the network. Even when disconnected, the user can still log in to that account.

Note: The mobile account's local home folder is deleted if you set account expiry settings and the account goes unused or if a local administrator deletes it. When the local home folder is deleted, the mobile account user can't log in away from the network.

The login window lists the mobile account based on the following:

- Login window settings
- The version of Mac OS X installed on your computers
- Whether the mobile account has a local home folder on the computer

For more information, see "Changing the Appearance of the Login Window" on page 201.

An *external account* is a special type of mobile account that is different from typical mobile accounts in the way users log in. For more information, see the next section.

Resolving Sync Conflicts

When a user's files and folders sync, a sync conflict can occur if a file in the user's local home folder and the network home folder have two versions of a file and it is not clear which one should be saved. Sync conflicts usually occur when a mobile account user changes files on one or more computers.

When sync conflicts occur, a dialog appears that allows the user to choose which version of a file to sync. The user can keep the files in the local or network home folder or keep both files.

The user can reset the sync history by pressing and holding the Shift and Option keys while logging in. When the sync information is reset and a sync conflict occurs, the sync conflict dialog reappears, asking which version of a file should be synced.

About External Accounts

An external account is a mobile account that has its local home folder stored on a volume in an external drive. The portable home directory is created from the local home folder stored on that external drive and the user's network home folder.

When the user connects an external drive containing his or her local home folder, the user can log in and use his or her account in the same way as if he or she had a mobile account with a local home folder on the computer. If the login window displays accounts in a list, the user can select his or her account, or if it has a name and password field, the user can enter his or her name and password.

External accounts require Mac OS X v10.5 or later and an external or ejectable volume that is formatted as Mac OS X Extended format (HFS Plus) or MS-DOS format (FAT).

If the external account is stored on a portable computer, the user must start target disk mode on the portable computer before connecting it to the client computer. When the portable computer is in target disk mode, all mobile accounts stored on it become external accounts.

After the user logs in, Mac OS X only shows the external account that the user logged in with. When the user views the account list in Accounts System Preferences, the user sees his or her external account but doesn't see other external accounts.

Similarly, the fast user switching menu displays all accounts with local home folders on the client computer. If the user chooses Login Window from the fast user switching menu, all external accounts are shown in the fast user switching login window.

Because their home folder is stored on an external volume, external account users can use File Sharing only when the external volume is present.

All mobile accounts on Mac OS X v10.5 or later (including external accounts) can use FileVault to encrypt the contents of the local home folder. For more information, see "Enabling FileVault for Mobile Accounts" on page 218.

For information about creating external accounts, see "Creating External Accounts" on page 221.

Logging In to External Accounts

If a user has a local home folder on an external drive and he or she connects it to a computer that allows the external account, logging in to an external account is like logging into a mobile account.

If there isn't a local home folder on the external drive, or if the external account isn't allowed, the user must take a few additional steps before he or she can log in with the external account. If the user has a local home folder on the computer, the user can't create a local home folder on an external drive.

If the user doesn't have a local home folder on an external drive, the location setting in mobile account creation options might give the user the choice of where to store the local home folder:

- If you set the location to "user chooses," a window appears allowing the user to choose where to store the local home folder. You can limit the choices to store on the computer or on an external drive, or you can choose both. If the user chooses an external drive, a local home folder is created on the external drive.
- If you set the location to "at path" and enter the path to the external drive, the user doesn't choose a location.

For more information about setting up mobile account creation options, see "Creating External Accounts" on page 221.

After a local home folder is created on the external drive, if the computer is connected to the directory server that holds the mobile account, the user is allowed to log in. If it's not connected to the directory server, Mac OS X checks to see if the external account is allowed or denied access to the computer.

If an external account isn't permanently allowed or denied access to a computer, a dialog appears asking if the external account should be allowed or denied access to the computer. To allow access, the user must authenticate as the local computer administrator.

If the external account is allowed access, the user logs in. If the user is denied access, the user is returned to the login window.

The local administrator can permanently allow or deny access to the computer. If a user is permanently denied access, he or she can hold down the Option key while logging in to redisplay the dialog.

Considerations and Strategies for Deploying Mobile Accounts

Before you deploy mobile accounts, carefully weigh the advantages and disadvantages of using them and strategize how you will configure them.

When you properly configure mobile accounts, you can create a work environment where users effortlessly access their latest files from several locations, keep their managed preferences while offline, and retrieve file backups if they lose or damage their computers, while requiring less network traffic than network accounts.

If improperly configured, mobile accounts can overload the server, force users to wait for long periods of time to log in or log out, and potentially cripple client computers by using all available hard disk space.

Advantages of Using Mobile Accounts

Mobile accounts have several advantages over using local or network accounts.

- Applications locally cache temporary files.
- Mobile accounts create less network traffic than network accounts.
- You can manage individual mobile accounts.
- Users can access their accounts and files when disconnected from the network.
- Users can recover data if their computers or external drives are lost or damaged.

Applications locally cache temporary files: When mobile account users run applications, those applications cache temporary files on the local computer. When external account users run applications, those applications cache temporary files on the external drive. When network account users run applications, instead of caching, the applications transfer temporary files over the network.

Because mobile accounts are not repeatedly transferring temporary files, they tend to be faster than other account types and also offer improved application stability. Some applications don't work with network home folders and temporary files that are not cached locally. Using mobile accounts, these applications run as if the user had a local account.

Mobile accounts create less network traffic than network accounts: When network account users save files, they transfer the files over the network. When they open files, they also transfer files over the network. With a mobile account, files are stored locally (on the client computer or in an external drive) and are only transferred during syncing.

Syncing only transfers files if the modification time of a local or network file is different than the last time the files synced.

Mobile accounts cache temporary files locally, improving network and individual computer performance. Caching files like webpages locally helps reduce network traffic.

You can also reduce network traffic by carefully planning user sync settings. For information about how to plan sync settings, see "Strategies for Syncing Content" on page 150.

You can manage individual mobile accounts: Like network accounts, you can use Workgroup Manager to manage preferences and set account attributes for individual mobile accounts.

You can manage users with local accounts only if you add a computer to a computer group. This allows you to set management preferences affecting all local accounts for that computer but it doesn't let you manage individual local accounts. To manage specific local accounts, you must log in to the local computers individually or use Apple Remote Desktop.

Users can access their accounts and files when disconnected from the network: Mobile accounts have two key features that allow users to access their accounts and files when disconnected from the network: cached authentication and portable home directories.

When mobile account users disconnect from the network using cached authentication, they can log in to the mobile account using the local home folder stored on the portable computer or on an external drive using the same login name and password they used when the computer or external drive was last connected.

By contrast, network account users can't access their accounts when they disconnect from the network. If you change the password for a user remotely, the next time the user connects to the network, he or she must use the new password to authenticate.

For information about portable home directories, see "About Portable Home Directories" on page 143.

Users can recover data if their computers or external drives are lost or damaged: If a user with a mobile account loses or damages his or her portable computer or external drive and logs in using a new computer, the server restores all previously synced files during the next sync.

Considerations for Using Mobile Accounts

Although mobile accounts provide many advantages over local and network accounts, they also have a few specific configuration needs that, if ignored, can create problems for network administrators.

Consider the following:

- Improperly set sync settings can cause long delays during login and logout and can create inconsistent home folders.
- If multiple users create a mobile account on the same computer, it could cause excessive proliferation of home folders.
- Mobile accounts can't restore deleted files through syncing.
- You can't create mobile accounts when connected to a network through a virtual private network (VPN) connection.

Improperly set sync settings can cause long delays during login and logout and can create inconsistent home folders: If you only sync large files at login and logout, this could significantly increase the amount of time it takes for users to log in and out. If users make changes to large files, they must wait for the files to sync before they can finish logging in or logging out.

If a number of users are making changes to large files and are simultaneously logging in to a wireless network with limited bandwidth, they can overload the network, further delaying their login.

If you do not sync key folders, this can create inconsistent home folders and confuse your users.

For example, as a school administrator, let's say you decide to only sync a student's ~/Documents folder. This means that if students don't save their homework in the ~/Documents folder, their homework isn't synced. When the students log in on another computer, they can't access their homework. Also, if homework saved in ~/Documents references pictures in ~/Pictures, the references might not work because the ~/Pictures folder is not synced.

If multiple users create a mobile account on the same computer, it could cause excessive proliferation of home folders: If you have a shared-access computer like a kiosk or lab computer, every time a user creates his or her mobile account, a local home folder is created. If unmanaged, this could completely fill the computer's available hard disk space.

If you set account expiry settings for a mobile account, you can automatically delete the local home folder after a period of inactivity. If you don't want to automatically delete the home folder, consider using network or generic local accounts, both of which prevent the user from creating local home folders.

If you set up a guest account, the contents of its local home folder are deleted when the user logs out.

Mobile accounts can't restore deleted files through syncing: Although mobile accounts keep user files stored in two locations—in local and network home folders—they do not eliminate the need for a formal backup system.

When you configure the user's portable home directory, you choose a subset of their folders to sync. This syncing affects files that are new, modified, or deleted since the last sync.

If users save files in locations that are not synced, the files remain local. If users delete files and then sync, those files are removed from local and network home folders.

Unlike some formal backup solutions, users can't retrieve older versions of files, such as versions saved prior to the last sync.

You can't create mobile accounts when connected to a network through a virtual private network (VPN) connection: You must create mobile accounts while being directly connected to the network. After enabling a mobile account, you can then use VPN to connect to the network and sync your mobile account.

Strategies for Syncing Content

Administrators can create a mobile account through Workgroup Manager, and users can create one through Accounts preferences. Each method has different sync capabilities:

- When you create a mobile account through Workgroup Manager, you can sync any folder in the user's home folder.
- When users create a mobile account, they can only sync top-level folders like ~/Desktop or ~/Documents.

A background sync occurs at a frequency set by you, or when the user manually syncs. By default, when you enable background syncing, it occurs every 20 minutes.

If a file in one home folder is modified and the file in the other home folder isn't, the newer file overwrites the older file. If both files have been modified since the last sync, the user chooses which file to keep.

Do not use background syncing with folders containing files accessed by multiple computers. This can cause users to load older, unsynced files. Examples:

- The user saves a file on one computer and loads the file on another computer. If the file was not synced to the server after its last save, the user loads an outdated version of the file from the server.
- The file might not exist on the server because it was not synced. If not, the user does not see the file or loads an outdated local version.
- The user uses the same mobile account to log in to two computers simultaneously. This can create sync issues with the computers, causing problems.

You should carefully manage login and logout syncing because of the delay caused by syncing. If a user has a slow network connection or is syncing many files or large files, the user must wait for syncing to complete before logging in or out.

To sync preference files such as the user's bookmarks and application preferences, use login and logout syncing. If you sync them in the background, newer files in the user's local home folder overwrite older files in the user's network home folder, but newer files in the user's network home folder aren't synced until the user logs in or out.

Consider syncing smaller files (such as preference files) at login and logout while syncing larger files (such as movies) in the background. This reduces login and logout times because only preference files sync, and movies sync throughout a user's session (instead of while the user is trying to log out). You can further reduce network traffic by choosing not to sync the movies folder, requiring users to access the movies folder locally.

By balancing login and logout syncing with background syncing, you can reduce the time required for logging in and logging out, while retaining consistent, synced home folders.

Setting Up Mobile Accounts for Use on Portable Computers

When distributing portable computers, you face challenges that don't apply when deploying stationary computers.

For example, to ensure your portable computers remain managed while off the network, you must give users mobile accounts and prevent them from creating their own local accounts, or from changing settings to bypass management.

Configuring Portable Computers

When you distribute portable computers to users, you must configure those computers to prevent users from circumventing your management scheme.

To set up portable computers for use on your network:

1. Install the operating system, applications, and utilities.

   Most computers come with Mac OS X installed. However, to install a newer version, make sure the computer meets the minimum requirements for installing the operating system, applications, and utilities.

2. Create local accounts on Mac OS X computers.

   Create at least one local administrator account and create local user accounts as needed. Make sure the users' local account names are not easily confused with the users' network names.

By creating an administrator account, you are preventing the user from having administrator access unless you specify it for that user. Administrator access allows the user to override many managed settings.

3 Set up computers and computer groups on your server.

Use Workgroup Manager to create computer accounts for portable computers and then add them to a computer group and enforce preference management for all users of those computers.

Computer group management does not always affect external accounts because external accounts can be used on computers that aren't connected to the network.

Allow the creation of mobile accounts for specific computers or computer groups rather than for specific users or groups. Doing so limits the creation of portable home directories only to specific computers. This way you can ensure that users who use several computers do not create portable home directories on each of those computers.

For more information about creating computer groups, see Chapter 6, "Setting Up Computers and Computer Groups." For instructions about creating mobile accounts, see "Creating a Mobile Account" on page 215.

Managing Mobile Clients Without Using Mobile Accounts

There are several situations in which you should not use mobile accounts for portable computer users. This section describes those situations and provides alternatives to using mobile accounts that allow you to manage portable computers.

Unknown Mac OS X Portable Computers

If a computer is connected to your network but is not in a computer group, it is considered to be an unknown or *guest* computer. If you can identify the unknown computer by its Ethernet ID, you can create a computer account for it so that it's no longer a guest computer.

You can use the guest computer account to manage guest computers on your network. This allows you to manage Mac OS X portable computers joining your directory domain. If guest computer users log in using network or mobile accounts, their user and group managed preferences and account settings apply.

For more information about how managed preferences interact when applied to users, groups, computers, and computer groups, see "Understanding Managed Preference Interactions" on page 167.

For more information about setting up a guest computer account for Mac OS X users, see "Working with Guest Computers" on page 116.

Using Mac OS X Portable Computers with One Primary Local User

You can also distribute portable computers with only local accounts and not assign mobile or network accounts to users. This can reduce or eliminate the burden of maintaining dedicated directory domain servers and servers that store home folders.

Even with local accounts, you can still manage users' computers when they use your network by adding their computers to a computer group.

When distributing portable computers, you can still retain control over the computer when the user logs in with a local account while off the network. To restrict a user from full use of the computer, do not assign him or her local administrator privileges.

You can also set parental controls to further control the computer while off the network. For more information about how to set parental controls, see Mac Help.

To restrict users from full access to a computer, create a local administrator account and a local user account on the computer. Give the user the login information for the local user account but not the local administrator account. Only administrator accounts allow users to install software and save or delete files outside of the home folder.

If you make a user the local administrator of a computer, you can deny him or her the ability to turn off your computer management. However, in many cases, the local administrator can still override management settings.

If local users want to share files with other users over the network, they can enable File Sharing in the Sharing pane of System Preferences and then use their ~/Public folder to share. Similarly, local users can connect to the computers of other users who have File Sharing enabled.

If users also have network accounts, you might prefer that they log in through their local accounts to reduce network traffic. They can connect to their network accounts through the "Connect to Server" command in the Finder Go menu.

Using Mac OS X Portable Computers with Multiple Users

Although mobile accounts are best suited for portable computers, there are a few situations in which using local accounts provides advantages over using mobile accounts.

For example, a school's wireless mobile lab might consist of 20 to 30 MacBooks, an instructor's computer, an AirPort Extreme Base Station, and a printer, all located on a mobile cart. Because all of these computers are on a mobile cart, the school could use this lab for multiple classrooms throughout the campus.

When using a wireless mobile lab, it is very difficult to control who uses specific computers. Unlike personal portable computers (where you know who uses which computer), or with stationary computers (where you can assign seating charts), it is hard to consistently use a distribution scheme for a wireless mobile lab. You could use stickers to label the computers and control distribution, but teachers would still need to monitor distribution to ensure students don't take the wrong computer.

When users create a portable home directory, they create a local home folder on the computer using some of the computer's hard disk space. If several dozen users create local home folders on a computer, you could run out of hard disk space for their files. You might have to set strict account expiry settings, depending on the amount of hard disk space on the computers and how many users use them.

Another consideration when using a wireless mobile lab is that the total network throughput is much more limited than a wired lab. If users have network accounts, when they open or save files it requires using the network, possibly slowing the network connections of other users.

Although mobile accounts help alleviate these issues, frequent syncing can also slow the network. Creating mobile accounts without synced folders efficiently utilizes the network. However, users must still copy and store files in their network home folders if they want to access their files from other computers.

To manage your cart's MacBooks, you might create generic local user accounts on each computer.

For example, you could create identical generic local user accounts on each computer (such as all accounts could have "Math" as the user name and "student" as the password), and then create different generic local accounts for each class (such as an account for a history class, one for a biology class, and so on). Each account has a local home folder but does not have administrator privileges.

To perform maintenance tasks and upgrades, install software, and administer local user accounts, you would use a separate local administrator account on each computer to allow server administrators (or other individuals).

If a generic configuration works for all users of a computer, instead of creating several generic local accounts, enable the guest account. To use the guest account, your computers must run Mac OS X v10.5 or later. The guest account is a local account that doesn't require a password and can't be logged into remotely. When a guest user logs out, all information and files in the guest account's home folder are deleted.

After creating local user accounts or enabling the guest account, you could then add each computer to a computer group and manage preferences for the computer or computer group.

Because multiple users can store items in the local home folder for a generic account, you might want to periodically clean out that folder as part of your maintenance routine.

You might also recommend that students save files to a network drop box to ensure their files are not deleted, and to allow them to access those files regardless of who uses the computer next.

Instead of using local accounts, you could use external accounts, which would give your users individual accounts (with separate home folders). For external accounts, each student needs an external drive. This eliminates the need for hard-disk-space management on the portable computers, and you don't have to set strict account expiry settings. This also allows you to manage at the level of users, groups, computers, or computer groups.

The biggest issue with using external accounts for a mobile lab cart scenario is sync-over-wireless. If you don't carefully set sync settings, the mobile accounts could sync very large files and overload the wireless network.

Securing Mobile Clients

Several security considerations for mobile clients do not exist for stationary clients. These considerations are relevant because of the mobility of the users' computers. When they are off your network, you can no longer monitor the actions of malicious users, nor can you control the network environment that your users join.

You can use FileVault to secure the local home folder of a mobile account. If an intruder accesses the computer storing the local home folder while the user isn't logged in, the intruder can't access the contents of the local home folder. For more information, see "Enabling FileVault for Mobile Accounts" on page 218.

Consider taking additional steps to improve your network security and client computer security. For information, see *Mac OS X Security Configuration* and *Mac OS X Server Security Configuration*.

Optimizing the File Server for Mobile Accounts

In Server Admin, you can enable an option called "Server Side File Tracking for Mobile Home Sync," which reduces the strain on a file server that occurs when mobile accounts sync.

When mobile accounts sync, the user's computer scans every folder in the local home folder and compares them with all folders in the network home folder. This scanning is unnecessary when only a few folders change and require syncing.

If you enable the option, a server daemon updates the database of changed files. The user's computer scans only the folders in the local home folder that have been modified since the last time the database was updated.

To enable the option, TCP port 2336 must be open on your file server's firewall.

To optimize the file server for mobile accounts:

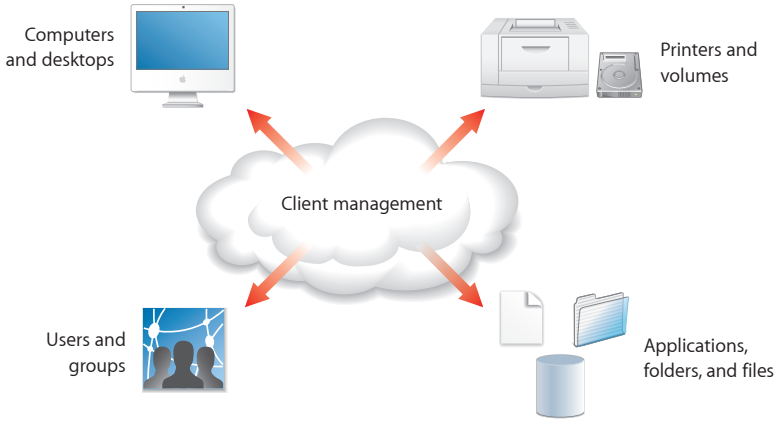
1. In Server Admin, click the disclosure triangle for the server hosting network home folders for mobile accounts.
2. If Firewall isn't listed, select the server, click Settings, click Services, select Firewall, and then click Save.
3. Select Firewall, click Settings, and then click Services.
4. Choose the address range for your users' computers from the "Edit Services for" pop-up menu.
5. Select "Allow only traffic from '*ipaddress*' to any of these ports," select the Allow checkbox for Mobile Account Sync (port 2336), and then click Save.
6. Select the server, click Settings, and then click General.
7. Select "Server Side File Tracking for Mobile Home Sync" and then click Save.

Client Management Overview

9

Use this chapter to learn about Mac OS X client management.

Client management is the centralized administration of your users' computer experience, as shown in the following illustration.



Client management is usually implemented by:

- Managing access to network printers and to server-resident home folders, group folders, and other folders.
- Customizing the computer work environment of users, groups, and computers by defining preferences for user accounts, group accounts, computers, and computer groups.

This chapter introduces each of these client management topics as they apply to users of Mac OS X computers.

Using Network-Visible Resources

Mac OS X Server lets you make various resources visible throughout your network so users can access them from different computers and various locations.

There are several key network-visible resources:

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

  A home folder contains several folders—such as Desktop, Documents, and Public—to help organize information. After logging in, users access their network home folders by clicking the Home icon in the Finder.

- **Group folders.** When you set up a group account for network users, you can associate a group folder with the group. A *group folder* is a place for group members to exchange information electronically. By default, it contains three folders—Documents, Library, and Public. The Public folder contains a Drop Box folder, which allows users to easily share their files.

  By residing on the server for easy access throughout the network, a group folder can be shown in the Dock for access from wherever a user wants to work on group activities.

- **Other shared folders.** You can set up other folders on the server to provide users with access to applications, handouts, announcements, schedules, and other files.

- **NetBoot and NetInstall images.** You can use NetBoot images and NetInstall images on the server to simplify the setup of network users' computers.

  A user's computer can start up from a *NetBoot image* stored on the server. You can use the same computer for a science lab booting from one image and for a French lab booting 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 did on the computer.

  A *NetInstall image* installs preconfigured software on users' computers, making it easy to remotely deploy the operating system, additional applications, and even custom computer settings, without user interaction.

Customizing the User Experience

You manage a network user's work environment by defining preferences—settings that customize and control the user's computer experience.

There are two panes in Workgroup Manager Preferences: Overview and Details. To manage predefined system preferences, use the Overview pane. To manage preferences for an application or utility that has a preference manifest, use the Details pane.

The Overview pane is identical for users and groups, but additional items (Energy Saver and Time Machine) appear for computers and computer groups.

Many factors, including user responsibilities and security issues, determine what computer work environment is most suitable for a user. In some cases, setting up informal usage guidelines is sufficient. In other cases, tightly controlling the computer experience is necessary, with each setting defined and each application controlled. The preferences you define should use Mac OS X capabilities that best support your user and your business requirements.

The Power of Preferences

Many preferences, such as Dock and Finder preferences, customize the appearance of the desktop. For example, you can set up Dock and Finder preferences so the user's work environment is simplified by including only essential applications and key folders in the Dock.

Other preferences manage what users 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.

The following table summarizes 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		✓	Applications a user can open
Classic	✓		Classic environment startup
Dock	✓		Appearance and contents of the Dock
Energy Saver	✓		Startup, shutdown, wake, sleep, and performance settings
Finder	✓	✓	Appearance of desktop icons and Finder elements
Login	✓		Login experience
Media Access		✓	Ability to use recordable media
Mobility	✓		Creation of mobile accounts
Network	✓	✓	Proxy settings for accessing servers through a firewall

This preference	Tailors the work environment	Limits access and control	By letting you manage
Parental Controls		✓	Web access and time limits on computer use
Printing		✓	Printers a user can use, and page footer settings
Software Update	✓		Server to use for updates
System Preferences		✓	System preferences that are enabled on the user's computer
Time Machine	✓		Which volumes are backed up and how long the backup files are retained
Universal Access	✓		Hardware settings for users with special visual, auditory, or other needs

Designing the Login Experience

An example of the power of preference management is the ability to shape and control the user's login experience. You can set up Login preferences for computers and computer groups to control the appearance of the login window.

The following table provides example configurations of the login window and login options to suit your environment.

Environment	Desired effect	Key login settings
Kiosk	The computer should always be logged in as a local or guest account. Users can also log in with their personal accounts (externally or by using network accounts).	• Show "Other" • Don't show Restart or Shut Down buttons • Don't show password hint • Enable automatic login • Don't enable >console login • Don't log out inactive users • Enable external accounts • Enable guest account
Educational lab	Users should be able to select their account from a list. People without accounts shouldn't be able to shut down or restart the computer. Inactive users should be automatically logged out.	• Message: "Welcome to the Math Lab." • Show mobile accounts and network users • Don't show Restart or Shut Down buttons • Don't show password hint • Don't enable automatic login • Log out inactive users • Enable external accounts
Corporate workstation	Users must enter their name and password to log in. Users should be able to work without being logged out. Except for primary users, no one can log in unless they have a network or local account.	• Message: "If you have issues, contact the IT help desk at ..." • Show name and password text fields • Show Restart and Shut Down buttons • Don't show password hint • Don't enable automatic login • Don't log out inactive users • Don't enable external accounts • Don't enable guest account

Environment	Desired effect	Key login settings
High security	The computer should be as secure as possible, restricting who can use the computer and how they log in.	• Message: "Unauthorized use prohibited" • Show name and password text fields • Don't show Restart or Shut Down buttons • Don't show password hint • Don't enable automatic login • Don't enable >console login • Don't enable fast user switching • Log out inactive users • Don't enable external accounts • Don't enable guest account

Choosing a Workgroup

In addition to customizing the login window, you can manage login preferences that affect whether users choose workgroups.

If you don't manage login access preferences, after the user authenticates, a list of available workgroups appears (depending on computer settings and if the user belongs to more than one workgroup).

Network account users choose from workgroups in their directory domain but local users access their workgroups from their local directory domain.

It's possible for a user to belong to a group that doesn't appear in the list. The login screen lists only workgroups that are allowed access by the computer group.

Local administrators also have the option not to choose a workgroup and disable preference management.

Users can select "Remember my choice," which bypasses the workgroup chooser in future logins and selects a workgroup for the user. Users can still change their workgroup by holding down the Option key while their password is validated.

If the computer or the computer group it's associated with supports local-only users, all workgroups that are given access to the computer by the computer group are listed after a local user logs in. The user can select from any of these.

Preferences associated with the user, the chosen workgroup, parent workgroups, and the computer being used, take effect upon login.

If you manage login access preferences, you can customize the workgroup choosing process. For example, you could:

- Ensure that the workgroup chooser is always shown (by selecting "Always show workgroup dialog during login," and in login options, deselecting "Local administrators may refresh or disable management").
- Bypass the workgroup chooser and combine settings from all available workgroups (by selecting "Combine available workgroup settings").
- Prevent parent group preferences from taking effect (by selecting "Ignore workgroup nesting").

For more information, see "Customizing the Workgroups Displayed at Login" on page 205.

Working with Synced Homes

After choosing a workgroup, users with local or network accounts are logged in. If the user has a mobile account, he or she might be prompted to create a synced home, depending on the user's mobility settings and whether he or she already has a mobile account.

After the user creates a synced home, he or she might be prompted to choose where to store the home. The user can choose a volume on the local computer or on an external volume, such as an external hard drive. If you choose the location for the user (by setting it to the startup volume or a specific path), the user won't need to choose where to create the home.

Like the login preferences set in Workgroup Manager, mobility preferences also affect how users log in and what dialogs are shown, and they dictate the kinds of decisions the user must make when they log in. By managing preferences, you choose what features are available and whether they're automatically enabled or the user must enable them.

Login and mobility preference management is an example of how preference management allows you to precisely sculpt the user experience.

Improving Workflow

You can use preference management to improve workflow by limiting the number of applications and folders that appear. You can also make applications and folders more accessible by putting them in the Dock and creating multiple workgroups (groups with managed preferences), each of which has a Dock that is customized to show only the applications used by users in the group.

Applications can be stored locally on a computer's hard disk or on a server in a share point. If applications are stored locally, users can find them in the Applications folder. If applications are stored in a share point and you don't add the share point as a login item, the user must connect to the server by choosing Go > Connect to Server in the Finder to locate and use applications.

Applications can also be made available through an automounted share point as the /Network/Applications mount record.

To make specific applications easy to find, you can use Dock Items preferences to place an alias for the My Applications folder in the user's Dock. The My Applications folder contains aliases for applications.

However, adding the My Applications folder might extend the login time for managed users because Mac OS X must search available disks to build the applications list for every login.

For instructions on creating aliases to My Applications and other folders in a user's Dock, see "Adding Items to a User's Dock" on page 187.

You can manage user access to local applications by creating lists of approved applications in the Applications preferences. (See "Allowing Legacy Users to Open Specific Applications and Folders" on page 179.) This list determines what users find in the My Applications folder located in the Dock.

To prevent users from opening a Finder window to easily browse to other applications, use Simple Finder. For more information about using Simple Finder, see "Setting Up Simple Finder" on page 193.

If you created a group folder, you can set up quick access to the folder when a user logs in to the workgroup associated with the folder. Users can use this group folder to facilitate file sharing between group members.

For instructions on creating an alias for the group folder, see "Providing Easy Access to Group Folders" on page 186. To provide access to the group volume, which contains the /Public folder and a drop box for the group, see "Providing Easy Access to the Group Share Point" on page 212.

Managing Preferences

10

Use this chapter to learn how to manage preferences for users, workgroups, computers, and computer groups.

By managing preferences for users, workgroups, computers, and computer groups, you can customize the user's experience and restrict user access to only the applications and network resources you choose.

To manage preferences, use the Preferences pane in Workgroup Manager.

For an overview of how to use managed preferences to customize the user experience, see "The Power of Preferences" on page 159, and "Designing the Login Experience" on page 160.

Using Workgroup Manager to Manage Preferences

Workgroup Manager allows you to set and lock specific system settings for users on the network. You can set initial preferences and allow users to change them later or you can keep preferences under administrative control at all times. (You can also leave preference settings unmanaged.)

Workgroup Manager provides control over most major system and application preferences, as well as settings for users, groups, computers, and computer groups. The preference editor controls the remainder of the applications that require management.

These preference panes allow you to manage the following settings:

Preference pane	What you can manage
Applications	Applications and Dashboard widgets available to users, and if Front Row is enabled. For more information, see "Managing Access to Applications" on page 175.
Classic	Classic startup settings, sleep settings, and the availability of Classic items such as Control Panels. For more information, see "Managing Classic Preferences" on page 180.
Dock	Dock location, behavior, and items. For more information, see "Managing Dock Preferences" on page 185.
Energy Saver	Performance options for Mac OS X client and server computers, battery usage for portable computers, and sleep or wake options. For more information, see "Managing Energy Saver Preferences" on page 188.
Finder	Finder behavior, desktop appearance and items, and availability of Finder menu commands. For more information, see "Managing Finder Preferences" on page 193.
Login	Login window appearance, mounted volumes, access control, scripts, and items that automatically open. For more information, see "Managing Login Preferences" on page 200.
Media Access	Settings for optical discs, internal and external disks, and disk images. For more information, see "Managing Media Access Preferences" on page 212.
Mobility	Creation of mobile accounts at login and mobile account options. For more information, see "Managing Mobility Preferences" on page 214.
Network	Configuration of specific proxy servers and settings for hosts and domains to bypass and disabling Internet Sharing, AirPort, and Bluetooth. For more information, see "Managing Network Preferences" on page 227.

Preference pane	What you can manage
Parental Controls	Content filtering or client computer usage limiting. For more information, see "Managing Parental Controls Preferences" on page 231.
Printing	Available printers, printer access, and page footers. For more information, see "Managing Printing Preferences" on page 234.
Software Update	Specific server to use for software update service. For more information, see "Managing Software Update Preferences" on page 238.
System Preferences	System preferences available to users. For more information, see "Managing Access to System Preferences" on page 239.
Time Machine	Time Machine settings like backup server location, and coverage. For more information, see "Managing Time Machine Preferences" on page 240.
Universal Access	Settings to control mouse and keyboard behavior, enhance display settings, and adjust sound or speech for users with special needs. For more information, see "Managing Universal Access Preferences" on page 241.

Understanding Managed Preference Interactions

You can define preferences for user accounts, group accounts, computers, and computer groups that are set up in a shared directory domain.

A user whose account has defined preferences is referred to as a *managed user*. An individual computer, or a computer that is a member of a computer group with defined preferences, is called a *managed computer*. A group with defined preferences is called a *workgroup*.

You can define Energy Saver, Time Machine, and Login preferences only for computers and computer groups, but you can define other preferences for users, workgroups, computers, and computer groups.

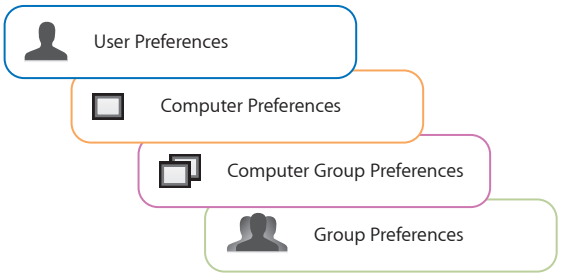
There are three types of managed-preference interactions:

- Printing, Login, Applications, System Preferences, and some Dock preferences (involving items that appear in the Dock) are considered *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 used.

- Other preferences defined at more than one level can be *overridden* at login.

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



When preferences that override conflict, user preferences override computer, computer group, and group preferences. Computer preferences override computer group and group preferences. Computer group preferences override group preferences.

For example, let's say you have different managed Dock preferences for users, workgroups, computers, and computer groups. The Dock preferences for the user take precedence, overriding and nullifying Dock preferences set for computers, computer groups, or workgroups. If you do not manage Dock preferences for the user, the computer and computer group Dock preferences override and nullify group Dock preferences.

An example of when preferences that override might be useful is in a school environment where you want to prevent students from using recording devices attached to a school computer, except for students who serve as lab assistants.

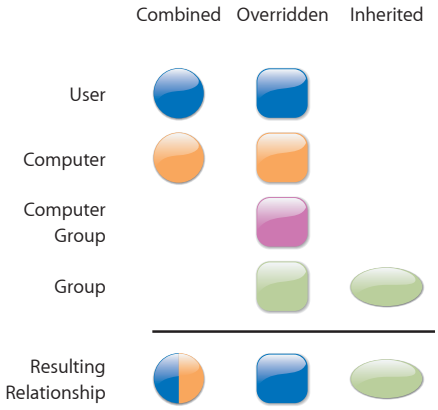
You could set up Media Access preferences for workgroups or computer groups to limit all students' access but override these restrictions for lab assistants using Media Access settings at their user account level. You could also designate a specific computer for media recording by overriding the restrictions at the computer level.

- *Inherited* preferences are preferences set at only one level.

  In some cases, it might be easier and more useful to set preferences at only one level.

  For example, you could set printer preferences only for computer groups, set application preferences only for workgroups, and set Dock preferences only for users. In this example, no overriding or combining occurs, and the user inherits the preferences without competition.

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



Most of the time you'll use workgroup-level and computer-group-level preferences:

- Workgroup preferences are most useful to customize the work environment (such as application visibility) for specific groups or to use group folders.

  For example, a student might belong to a group "Class of 2011" for administrative purposes and to a workgroup "Students" to limit application choices and provide a group shared folder for turning in homework. Another workgroup might be "Teacher Prep," used to provide faculty members with access to folders and applications for their use only.

- Computer-group-level preferences are useful when you want to manage preferences for users regardless of group associations. At the computer-group level, you might want to limit access to System Preferences, manage Energy Saver and Time Machine preferences, list specific users in the login window, and prevent the saving of files and applications to recordable discs.

  Computer group preferences also offer a way to manage the 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.)

  To manage local accounts, set up a computer group that supports local-only accounts. Preferences associated with the computer group and with any workgroup a user selects during login take effect.

Understanding Hierarchical Preference Management

Mac OS X Server v10.5 or later includes managed *hierarchical groups*—groups composed of nested groups, and computer groups composed of nested computer groups. By managing preferences for a parent group or computer group, child or computer groups also receive these managed preferences.

Child preferences take precedence and can override parent preferences. For example, Dock settings set for a child override Dock settings set for a parent.

Combined preferences come from the child and parent. For example, if you make a printer available for a parent group and a different printer available to a child group, a user who belongs to the child group can access both printers.

Be careful when creating situations where a child has several parents. If you don't manage an overriding preference for a child and you have conflicting overriding preferences for several of the child's parents, it is hard to predict which parent's preference takes precedence.

Combined preferences work even when children have several parents. The preferences of all parents combine with the child's preferences.

Don't make a child a parent of one of its parents. When you do you create a loop—where a child is its own grandparent—which introduces unpredictable behavior.

Setting the Permanence of Management

When you define preferences, you can manage them Always or Once. They are set to Never by default:

- *Always* causes the preferences to remain in effect until you change them on the server. When properly designed, a Mac OS X application that conforms to standard preference conventions does not allow a user to modify preferences set to Always. You can use Always to ensure users can't add or remove Dock items.

  Some applications might allow the user to change the Always managed preference, but the next time the user logs back in, the preference reverts to the managed setting.

- *Once* is available for some preferences. You can create default preferences, which users can then modify and keep the modifications. These preferences are effectively unmanaged.

  For example, you could set up a group of computers to display the Dock in a specific way the first time users log in. A user can change these preferences (you've set to Once) and the selected changes always apply to that user.

  In the Overview Preference panes, you can set the following preferences to Once: Dock, Finder (Preferences and Views), Login (Login Items), Mobility (Login & Logout Sync and Background Sync panes of Rules), and Universal Access. For all other preferences, you must choose Always or Never.

- *Never* lets a user control his or her preferences. However, some preference settings, such as Accounts and Date & Time, require a local administrator's name and password before changes can be made.

Never also means that the preferences are not managed at this account level but might be managed at a different account level. For example, even if you set the Dock preference to Never for a user, the Dock preference could still be managed at the group or computer level.

Note: When using the preference editor (the Details view in the Preferences pane), you can set preferences to *Often*. Often settings are similar to Once settings, but are reapplied at every login. This management setting is useful for training environments.

Users can customize their preferences to suit their needs during a session without any risk of affecting a future user's work experience. Some applications only respond to preference management set to Often.

Caching Preferences

Preferences are cached on Mac OS X computers so they remain in effect even when the computer is off the network. With Mac OS X v10.5 and later, the preferences cache is automatically managed:

- Computer preferences and preferences for workgroups that can use the computer are cached.
- User preferences are always cached for users who have mobile accounts.

When a computer is off the network, only users with local accounts or network users with mobile accounts on that computer can log in.

Preference Management Basics

In Workgroup Manager, information about users, groups, computers, and computer groups 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 specific 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 an Open Directory domain.

Preferences are stored in a user, group, or computer record. During login, the managed client combines them into a management list that is applied to the user experience.

After user accounts, group accounts, computer accounts, and computer groups are created, you can manage preferences for them using the Preferences pane in Workgroup Manager.

To manage preferences for Mac OS X clients, make sure that each user you want to manage has a network home folder or a local home folder on the server.

For information about how to set up home folders for users, see Chapter 7, "Setting Up Home Folders"

Note: When you manage preferences for a user, group, or computer, an arrow icon appears next to the managed preference in the Preferences pane to indicate that you're managing that preference. You can select multiple users, groups, or computers to review managed preferences. If the arrow icon is dimmed, it means managed preference settings are mixed for the selected items.

Managing User Preferences

You can manage preferences for users as needed. However, if you have large numbers of users, it can be more efficient to manage most preferences by group and computer. You might want to manage preferences at the user level only for specific individuals, such as directory administrators, teachers, or technical staff.

Consider which preferences you want to leave under user control. For example, if you aren't concerned about where a user places the Dock, you might want to set Dock Display management to Never or Once.

To manage user preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Click the Users button and select one or more user accounts from the list.
4. Click the icon for the preference you want to manage.
5. In each Preference pane, select a Manage option.

   In Media Access, the management setting applies to all preferences rather than to individual panes.
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 for some types of accounts.
7. When you finish, 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 user can save time, especially when you have large numbers of managed users.

Because users can select a workgroup at login, they can choose a group with managed settings related to the current task, location, or environment. It can be more efficient to set preferences once for a single group instead of setting preferences for each member of the group.

To manage group preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Click the Groups button and select one or more group accounts from the list.
4. Click the icon for the preference you want to manage.
5. In each preference pane, select a Manage option.

   In Media Access, the management setting applies to all preferences rather than to individual panes.
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 for some types of accounts.
7. Click Apply Now.

Managing Computer Preferences

Computer preferences are preferences set for individual computers.

Energy Saver and Time Machine preferences can be managed for computers and computer groups, but not for users or groups.

To manage computer preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Click the Computers button and select one or more computers.
4. Click the icon for the preference you want to manage.
5. In each preference pane, select a Manage option.

   In Media Access, the management setting applies to all preferences rather than to individual panes.
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 for some types of accounts.

7 Click Apply Now.

Managing Computer Group Preferences

Computer preferences are shared among all computers in a computer group. In some cases, it is more useful to manage preferences for computers rather than users or groups.

Energy Saver and Time Machine preferences can be managed for computers and computer groups, but not for users or groups.

To manage computer group preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3 Click the Computer Groups button and select one or more computer groups.

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

5 In each preference pane, select a Manage option.

In Media Access, the management setting applies to all preferences rather than to individual panes.

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 for some types of accounts.

7 Click Apply Now.

Disabling Management for Specific Preferences

After you set managed preferences for an account, you can turn off management for specific preference panes by changing the management setting to Never.

You can use the Once setting to create default settings. These are settings that, when saved, take effect the next time users log in. Users can then modify their settings and save their modified settings for future use.

To selectively disable preference management:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

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

5 In the pane with the preferences you no longer want to manage, select Never.

In Media Access, the management setting applies to all preferences rather than to individual panes.

6 Click Apply Now.

Setting the management setting to Never disables management for the current level in the users, computers, or groups hierarchy. Preferences can still be managed at a different level.

When you change the preference management settings, the new settings apply to all items in the active preference pane. To disable all management for an individual preference (for example, Dock), make sure the management setting is set to Never in each pane of that preference.

Managing Access to Applications

Use Applications preferences to allow or restrict user access to applications.

Computers identify applications using digital signatures (used in Mac OS X v10.5 or later) and bundle IDs (used in Mac OS X v10.4 or earlier, but can be used in Mac OS X v10.5 or later).

Digital signatures are more secure because clever users can manipulate bundle IDs. Workgroup Manager supports the use of both methods.

Use the Applications pane to work with digital signatures. Use the Legacy pane to work with bundle IDs.

Application restrictions depend on which pane you're managing and the version of Mac OS X run by client computers:

- If you manage the Applications pane and your users run Mac OS X v10.5 or later, Applications settings take effect and Legacy settings are ignored.
- If you don't manage the Applications pane, Legacy settings take effect for any version of Mac OS X.
- If your users run Mac OS X v10.4 or earlier, only Legacy settings take effect.

You can also use settings in Applications preferences to allow only specific widgets in Dashboard or to disable Front Row.

The table below describes what the settings in each Applications pane can do.

Applications preference pane	What you can control
Applications	Access to specific applications and paths to applications using digital signatures (for users of Mac OS X v10.5 or later)
Widgets	List of allowed Dashboard widgets (for users of Mac OS X v10.5 or later)
Front Row	Whether Front Row is allowed
Legacy	Access to specific applications and paths to applications using bundle IDs (primarily for users of Mac OS X v10.4 or earlier)

Controlling User Access to Specific Applications and Folders

You can use Workgroup Manager to prevent users from launching unapproved applications or applications located in unapproved folders.

In Mac OS X v10.4 or earlier, applications were identified by their bundle IDs. If your users have Mac OS X v10.5 or later installed, you can use digital signatures to identify applications. Digital signatures are much more difficult to circumvent than a bundle ID.

Workgroup Manager can sign applications that aren't already signed. When signing an application, you can embed a signature or you can store a detached signature separate from the application.

Embedding a signature has several performance benefits over a detached signature, but with signature embedding you must make sure every computer has the same signed application. For applications that are run from a CD, DVD, or other read-only media, you must use detached signatures.

Workgroup Manager uses the following icons to identify the kind of signature associated with an application.

Icon	Indicates the application has this type of signature
(no icon)	Embedded signature
	Detached signature
	No signature

Applications that include helper applications are identified by a disclosure triangle. When you click the disclosure triangle, you see a list of helper applications. By default, these helper applications are allowed to open.

You can disable individual helper applications, but the application might behave erratically if it requires the helper applications.

To allow or prevent users from launching an application, add the application or application path to one of three lists:

- **Always allow these applications.** Add applications that should always be allowed, regardless of their inclusion in other lists. You can sign applications added to this list. Don't add unsigned applications to this list because they allow users to disguise unapproved applications as approved applications.
- **Disallow applications within these folders.** Add applications and folders containing applications you want to prevent users from opening. All applications in the subfolders of a disallowed folder are also disallowed. Disallowing a folder within an application package can cause the application to behave erratically or fail to load.
- **Allow applications within these folders.** Add applications and folders containing applications you want to allow. All applications in the subfolders of an allowed folder are also allowed. Unlike applications in the "Always allow these applications" list, applications listed here are not allowed if they or their paths are listed in the "Disallow applications within these folders" list.

If an application or its folder doesn't appear in these lists, the user can't open the application.

To allow users to open specific applications and folders:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Applications and then click the Applications tab.
5. Set the management setting to Always.
6. Select "Restrict which applications are allowed to launch."
7. Click the Applications tab (within the Applications pane), click the Add (+) button, choose an application you want to always allow, and then click Add.

   When you allow an application, you also allow all helper applications included with that application. You can deselect helper applications to disallow them.
8. If you're asked to sign the application, click Sign; if you're asked to authenticate, authenticate as a local administrator.

   To add the application to the list as an unsigned application, click Don't Sign.

   When you sign the application, Workgroup Manager tries to embed the signature. If you don't have write access to the application, Workgroup Manager creates a detached signature.

While signing an application, you might be asked to authenticate as an administrator of the computer running Workgroup Manager.

9 Click the Folders tab, click the Add (+) button next to "Disallow applications within these folders," and then choose folders containing applications you want to prevent users from launching.

10 Click the Add (+) button next to the "Allow applications within these folders" field and choose folders containing applications you want to allow.

Disallowing folders takes precedence over allowing them. If you allow a folder that is a subfolder of a disallowed folder, the subfolder is still disallowed.

11 Click Apply Now.

Allowing Specific Dashboard Widgets

If your users have Mac OS X v10.5 or later installed, you can prevent them from opening unapproved Dashboard widgets by creating a list of approved widgets (which can include widgets included with Mac OS X and third-party widgets). To approve third-party widgets, you must be able to access them from your server.

To allow specific Dashboard widgets:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Applications and then click Widgets.

5 Set the management setting to Always.

6 Select "Allow only the following Dashboard widgets to run."

7 To allow specific widgets, click the Add (+) button, select the widget's .wdgt file, and then click Add.

The widgets included with Mac OS X are in /Library/Widgets.

8 To prevent users from opening specific widgets, select the widget and click the Remove (–) button.

9 Click Apply Now.

Disabling Front Row

With Workgroup Manager, you can disable Front Row.

To disable Front Row:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Applications and then click Front Row.

5 Set the management setting to Always.

6 Deselect Allow Front Row.

7 Click Apply Now.

Allowing Legacy Users to Open Specific Applications and Folders

To control user access to applications in Mac OS X v10.4 or earlier, you either:

- Provide access to a set of approved applications that users can open
- Prevent users from opening a set of unapproved applications

You can also set additional options to further control user access to applications.

When users have access to local volumes, they can access applications on the computer's local hard disk. If you don't want to allow this, you can disable local volume access.

Applications use helper applications for tasks they can't complete independently. For example, if a user tries to open a web link in a mail message, the mail application might need to open a web browser to display the webpage.

Disallowing helper applications improves security because an application can designate any other application as a helper application. However, you might want to include common helper applications in the approved applications list. This avoids problems such as users being unable to open and view mail content or attached files.

Occasionally, applications or the operating system might require the use of UNIX tools, such as QuickTime Image Converter. These tools can't be accessed directly and generally operate in the background without the user's knowledge. If you disallow access to UNIX tools, some applications might not work.

Allowing UNIX tools enhances application compatibility and efficient operation, but might decrease security.

If you don't manage Applications settings for computers running Mac OS X v10.5 or later, Legacy settings are used.

To set up a list of accessible applications:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3. Select one or more users, groups, computers, or computer groups.
4. Click Applications and then click Legacy.
5. Set the management setting to Always.
6. Select "User can only open these applications" or "User can open all applications except these."
7. Add items to or remove items from the list.

   To select multiple items, hold down the Command key.
8. To allow access to applications stored on the user's local hard disk, select "User can also open all applications on local volumes."
9. To allow helper applications, select "Allow approved applications to launch non-approved applications."
10. To allow use of UNIX tools, select "Allow UNIX tools to run."
11. Click Apply Now.

Managing Classic Preferences

You use Classic Preferences to set Classic startup options, assign a Classic System Folder, set sleep options for the Classic environment, and make specific Apple menu items available to users.

The Classic System Folder is a Mac OS 9 System Folder that contains the Mac OS 9 operating system. When users run Classic applications, they are running Mac OS 9 from the Classic System Folder.

Classic can be run on Mac OS X v10.4 or earlier.

The table below describes what the settings in each Classic pane can do.

Classic preference pane	What you can control
Startup	Which folder is the Classic System Folder and what occurs 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 work with applications that run in Classic, it is convenient to have Classic start up immediately when a user logs in. If users rarely need Classic, you can have Classic start only when a user opens a Classic application or when a document requires such an application.

You can also choose to display an alert when Classic starts, giving users the option to cancel Classic startup.

To work with startup options for Classic:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Classic and then click Startup.
5. Set the management setting to Always.
6. To start Classic immediately when a user logs in, select "Start up Classic at login."

   When Classic starts up at login, the startup window is hidden and the user can't cancel Classic startup.

   If users rarely use Classic, you can deselect this option and Classic starts up when a user opens a document or an application requires it. In this case, the Classic startup window is visible to users and they can cancel Classic startup.
7. To show an alert dialog only when Classic starts up after a user attempts to open a Classic application or document, select "Warn at Classic startup."

   If users manually start Classic or if Classic starts up at login, the warning is not shown.

   Users can allow Classic startup to continue or they can cancel the process. If you don't want to allow users to interrupt Classic startup, deselect this option.
8. Click Apply Now.

Choosing a Classic System Folder

In most cases, there is only one Mac OS 9 System Folder on a computer, and it is on the Mac OS X startup disk. In this case, you don't need 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 receive an error message and can't 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 on a different disk, enforce the use of a specific folder when Classic is in use. It is important if you specify a path to the folder's location that all clients 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 settings in the Startup pane of the Classic preference, users can choose from among available Mac OS 9 System Folders (if they have access to the Classic pane of System Preferences).

To choose a specific Classic System Folder:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Classic and then click Startup.
5. Set the management setting to Always.
6. In the "Use this System Folder when Classic starts" field, enter the path to the Classic System Folder (for example, /Volumes/*VolumeName*/System Folder/), or click Choose and then browse to the folder you want.

   Make 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.
7. Click Apply Now.

Allowing Special Actions During Restart

If managed users have access to the Classic pane of System Preferences, they can click the Start/Restart button in the Classic pane to start or restart Classic.

You can allow users to perform special actions, such as turning off extensions, starting or restarting Classic, or rebuilding the Classic desktop file, from the Advanced pane of Classic system preferences. You might want to allow this for specific users, such as members of your technical staff.

To allow special actions during restart:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.

4 Click Classic and then click Advanced.

5 Set the management setting to Always.

6 Select "Allow special startup modes."

7 To allow users to rebuild the Classic desktop file, select "Allow user to rebuild Desktop."

Deselecting this option disables the Rebuild Desktop button in the Advanced pane of Classic system preferences.

8 Click Apply Now.

Controlling Access to Classic Apple Menu Items

Classic managed preference options allow you to control access to specific items in the Classic Apple menu, including Mac OS 9 control panels, the Chooser and Network Browser, and other Apple menu items. You can show or hide all, some, or none of these items in the Apple menu.

If an item is hidden, users can't access that item from the Apple menu. However, there might be alternative methods of access, such as starting the Chooser by navigating to it in 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 specify the applications a user can open. For more information, see "Managing Access to Applications" on page 175.

Note: Disallowing access to the Chooser can affect what happens when a user attempts to print from Classic (if printer management is also enforced). If users can't access the Chooser, they can't set up new printers or switch between types of printers (such as PostScript and non-PostScript printers).

To hide or show items in the Apple menu:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Classic.

5 Click Advanced and then set the management setting to Always.

6 To remove the Chooser and Network Browser from the Apple menu, select "Hide Chooser and Network Browser."

Deselect this option to show Chooser and Network Browser.

7 To remove Control Panels from the Apple menu, select Hide Control Panels.

Deselect this option to show Control Panels.

8 To hide remaining Apple menu items, select "Hide other 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 enters sleep mode to reduce the 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 might take a little longer.

In some circumstances, you might need to use applications that operate in the background without the user's interaction or knowledge. If a background application is in use when Classic enters sleep mode, that application suspends its activity. To keep the application running, set the Classic sleep setting to Never.

To adjust Classic sleep settings:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Classic.

5 Click Advanced and then set the management setting to Always.

6 Drag the slider to set the length of time 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 a user's Mac OS 9 preferences data in the Mac OS 9 System Folder. If a user has more than one computer, or if multiple users work on the same computer, 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 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 data. In this case, users share preferences. Changes made by the last user are in effect when the next user logs in.

To choose where Classic user preferences are stored:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Classic.

5 Click Advanced and then set the management setting to Always.

6 To maintain consistent Classic preferences, select "Use preferences from home folder."

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 in each Dock pane can do.

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

Controlling the User's Dock

Dock settings allow you to adjust the position of the Dock on the desktop and change the Dock's size. You can also control animated Dock behaviors.

To set how the Dock looks and behaves:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Dock and then click Dock Display.

5 Set the management setting to Once or Always.

6 Drag the Dock Size slider to make the Dock smaller or larger.

7 If you want items in the Dock to be magnified when a user moves the pointer over them, select Magnification and then adjust the slider.

Magnification is useful if you have many items in the Dock.

8 From the "Position on screen" radio buttons, select whether to place the Dock on the left, right, or bottom of the desktop.

9 From the "Minimize using" pop-up menu, choose a minimizing effect.

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

11 If you don't want the Dock to be visible all the time, select "Automatically hide and show the Dock."

When the user moves the pointer to the edge of the screen where the Dock is located, the Dock appears.

12 Click Apply Now.

Providing Easy Access to Group Folders

After you set up a group folder, you can make it easy for users to locate the group folder by placing an alias in the user's Dock. The group folder contains the group's Library folder, Documents folder, and Public folder (including a drop box). If you need help setting up a group share point, see "Creating a Group Folder" on page 111.

If the group folder 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 can't manage this setting for users or computers.

To add a Dock item for a group folder:

1 If you haven't set up a group share point, do so before proceeding.

2 In Workgroup Manager, click Preferences.

3 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

4 Click the Groups button and select one or more group accounts from the list.

5 Click Dock and then click Dock Items.

6 Set the management setting to Once or Always.

If you select Once, the group folder icon appears in the user's Dock initially, but the user can remove it.

7 Select "Add group folder."

8 Click Apply Now.

If you change the location of the group share point, 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.

Make sure you use consistent paths for items you add in the Dock. This is especially important if you add items in nonstandard locations (for example, putting an application in another folder besides /Applications). If the Dock item can't be found, a question mark replaces the item in the user's Dock.

To add items to a user's Dock:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Dock and then click Dock Items.
5. Set the management setting to Once or Always.

   If you select Once, the user can add and remove Dock items. If you select Always, the user can't remove items from the Dock.
6. To add applications, folders, and documents to the Dock, click the Add (+) button to browse and select the item you want.

   To remove a Dock item, select it and then click the Remove (–) button.

   You can rearrange Dock items in the list by dragging them into the order you want them to appear. Applications are always grouped at one end, while folders and files are grouped at the other. User-added items are located after your listed applications.
7. To add the My Applications folder, select My Applications.

   The My Applications folder contains aliases for approved applications listed in the Applications preference pane. If you do not manage the Applications preference, available applications are shown. If you enable Simple Finder, you should display the My Applications folder.
8. To add the Documents folder, select Documents.

   The Documents folder is located in the user's home folder.
9. To add the Network Home folder, select Network Home.

   The Network Home folder is the network home folder for users with network accounts. For users of mobile accounts, selecting Network Home adds the user's network home folder (not the user's local home folder) to the Dock.
10. To replace the user's current Dock with your selected items, deselect "Merge with user's Dock."
11. After you finish adding Dock items, click Apply Now.

Preventing Users from Adding or Deleting Dock Items

Ordinarily, users can add items to their own Docks, but you can prevent this. Users can't remove items you add to the Dock if you set the management setting to Always.

To prevent users from adding items to their Docks:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Dock and then click Dock Items.
5. Set the management setting to Always.
6. Deselect "Merge with user's Dock."
7. Click Apply Now.

Managing Energy Saver Preferences

Energy Saver preference settings help you save energy and battery power by managing wake, sleep, and restart timing for servers and client computers.

You can configure Energy Saver preferences for desktop and portable computers. Desktop and portable computers differ in that portable computers can run on battery power.

The table below summarizes what you can control with settings in each Energy Saver pane.

Energy Saver preference pane	What you can control
Desktop	Sleep timing for the computer, display, hard disks, and wake and restart options for Mac OS X and Mac OS X Server
Portable	Processor performance setting, sleep timing similar to Desktop, and wake and restart options for adapter and battery power sources
Battery Menu	Display of the battery status indicator
Schedule	Regular schedules for startup or shutdown

Using Sleep and Wake Settings for Desktop Computers

Putting a computer to sleep saves energy because it turns off the display and stops the hard disk from running. Waking up from sleep is faster than starting up your computer.

You can use the Energy Saver preference settings to put computers to sleep after a specified period of inactivity. Other settings enable you to wake or restart the computer when specific events happen.

To set sleep and wake settings:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Energy Saver and then click Desktop.
5. From the OS pop-up menu, choose Mac OS X or Mac OS X Server and set the management setting to Always.
6. To adjust sleep settings, choose Sleep from the Settings pop-up menu and choose from the following:

To do this	Do this
Set the length of time the desktop computer waits to enter sleep mode	Move the "Put the computer to sleep when it is inactive for" slider. The computer does not enter sleep mode if the slider is set to Never. The default setting for Mac OS X is 10 minutes. The default setting for Mac OS X Server is Never.
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 can't be longer than the computer's sleep setting. The default setting for Mac OS X is five minutes. The default setting for Mac OS X Server is 30 minutes.
Put the hard disks to sleep during periods of inactivity	Select "Put the hard disk(s) to sleep when possible."

7. To set wake and restart settings, choose Options from the Settings pop-up menu and choose from the following:

To do this	Do this
Wake the computer when the modem is activated	Select "Wake when the modem detects a ring."
Wake the computer when an administrator attempts remote access	Select "Wake for Ethernet network administrator access."
Alllow users to press the power button (without holding it down for a prolonged period) to put the computer in sleep mode	(For client computers with Mac OS X v10.3 or later) Select "Allow power button to sleep the computer."
Make sure the computer restarts if the power fails	Select "Restart automatically after a power failure." Deselect this option to disable automatic restart.

8 Click Apply Now.

To manually wake up a sleeping computer or display, the user can click the mouse or press a key on the keyboard.

Setting 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 (an adapter or a battery). You can also set the computer to restart if power suddenly fails.

To manage portable computer settings:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3 Select one or more computers or computer groups.

4 Click Energy Saver and then click Portable.

5 From the Power Source pop-up menu, choose Adapter or Battery and set the management setting to Always.

6 To adjust sleep settings, choose Sleep from the Settings pop-up menu and choose from the following:

To do this	Do this
Set the length of time the desktop computer waits to enter sleep mode	Move the "Put the computer to sleep when it is inactive for" slider. The computer does not enter sleep mode if the slider is set to Never. The default setting for adapter power supplies is 10 minutes. The default setting for battery power supplies is five minutes.
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 can't be longer than the computer's sleep setting. The default setting for battery and adapter power supplies is five minutes.
Put the hard disks to sleep during periods of inactivity	Select "Put the hard disk(s) to sleep when possible."

7 To set wake and restart settings, choose Options from the Settings pop-up menu and choose from the following:

To do this	Do this
Wake the computer when the modem is activated	Select "Wake when the modem detects a ring."
Wake the computer when an administrator attempts remote access	Select "Wake for Ethernet network administrator access."
Make sure the computer restarts if the power fails	Select "Restart automatically after a power failure." Deselect this option to disable automatic restart.
Choose the level of processor performance	In the Processor Performance pop-up menu, select Highest, Automatic, or Reduced. For computers using an adapter, the recommended setting is Highest. For computers using a battery, the recommended setting is Automatic.

8 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 to Users

Portable computers use a battery as a direct power source while disconnected from external power or as a backup power source while connected to external power.

When battery power is too low for the computer to function, the computer puts itself to sleep to conserve energy. When a user reconnects the computer to a functional power source (for example, by inserting a fresh battery or connecting a power adapter), the user can wake the computer and begin working again.

Users should be encouraged to monitor battery status when not connected to external power and use a power adapter when possible to maintain a fully charged battery.

To show battery status in the menu bar:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Energy Saver and then click Battery Menu.
5. Set the management setting to Always.
6. To display the battery status, select "Show battery status in the menu bar"; to disable the battery status, deselect this option.
7. Click Apply Now.

Scheduling Automatic Startup, Shutdown, or Sleep

You can schedule when 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 business hours, on weekends, or after a class is finished.

Scheduling automatic startup allows you to conveniently prepare a lab or classroom for immediate use.

To schedule automatic actions:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Energy Saver and then click Schedule.
5. From the OS pop-up menu, choose Mac OS X or Mac OS X Server and set the management setting to Always.

6 To schedule automatic startup, select "Start up the computer," choose a day or range of days (Weekdays, Weekends, or Every Day) from the pop-up menu, and then enter a time in the time field.

To disable scheduled startup, deselect this option.

7 To schedule automatic sleep or shutdown, select the checkbox, choose Sleep or Shut Down from the pop-up menu, choose a day or range of days (Weekdays, Weekends, or Every Day) from the pop-up menu, and then enter a time in the time field.

To disable scheduled sleep or shutdown, deselect this option.

8 Click Apply Now.

Managing Finder Preferences

You can control various aspects of Finder menus and windows, which can help improve or control workflow.

For example, you can simplify the user experience by enabling Simple Finder. You can also prevent users from writing to or ejecting disks.

The table below summarizes what you can do with each Finder preference pane.

Finder preference pane	What you can control
Preferences	Finder window behavior, Simple Finder, whether open items appear on the desktop, filename extension visibility, and the Empty Trash warning.
Commands	Whether commands in Finder menus and the Apple menu are available to users. These allow users to perform tasks such as connecting to servers or restarting the computer.
Views	The arrangement and appearance of items on a user's desktop, in Finder windows, and in the top-level folder of the computer.

Setting Up Simple Finder

You can select the normal Finder or Simple Finder as the user environment:

- The normal Finder looks and acts like the standard Mac OS X desktop.
- Simple Finder removes the ability to use a Finder window to access applications or modify files. This limits users' access to only what is in the Dock.

If you enable Simple Finder, users can't mount network volumes, create folders, or delete files.

In addition to using Workgroup Manager, you can use System Preferences to set up Simple Finder on a local computer. When you use Workgroup Manager to apply the Simple Finder environment and the feature is not in use on the local computer, only the client's Finder is affected. Dock and Application access settings must be managed separately.

You can set up Simple Finder on the local computer and use the application and Dock management features in Workgroup Manager to add Dock items and application access.

Important: Don't turn on Simple Finder for users who run Mac OS X v10.2 through v10.2.8 and log in to a workgroup with its own group folder. These users can't use applications because Simple Finder prevents access to the group folder.

To turn on Simple Finder:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Finder, click the Preferences tab, and then select a management setting.

   If you select Always, choose "Use normal Finder" or "Use Simple Finder."

   If you select Once, the account uses only the normal Finder.
5. Click Apply Now.

Keeping Disks and Servers from Appearing on the User's Desktop

Normally when a user inserts an external 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.

Disks and servers still appear in the top-level folder when a user clicks the Computer icon in a Finder window's toolbar.

To hide disk and server icons on the desktop:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Finder, click the Preferences tab, and then select a management setting.
5. Under "Show these items on the Desktop," deselect the items you want to hide.

6 Click Apply Now.

Controlling the Behavior of Finder Windows

You can select which folder appears when a user opens a new Finder window. You can also define how contents are displayed when a user opens folders.

To set Finder window preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click the Preferences tab, and then select a management setting.

5 Under "New Finder window shows," choose the default folder for the Finder window.

Select Home to show items in the user's home folder.

Select Computer to show the top-level folder, which includes local disks and mounted volumes.

6 To display folder contents in a separate window when a user opens a folder, select "Always open folders in a new window."

Normally, Mac OS X users can browse through a series of folders using a single Finder window.

7 To maintain a consistent view across windows, select "Always open windows in column view."

8 Click Apply Now.

Hiding the Alert Message When a User Empties the Trash

Normally, a warning appears when a user empties the Trash. If you don't want users to see this message, you can turn it off.

To hide the Trash warning message:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click the Preferences tab, and then select a management setting.

5 Deselect "Show warning before emptying the Trash."

6 Click Apply Now.

Making Filename Extensions Visible

A filename extension usually appears at the end of a filename (for example, .txt or .jpg). Applications use the filename extension to identify the file type.

To make filename extensions visible:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Finder, click the Preferences tab, and then select a management setting.
5. Select "Always show file extensions."
6. Click Apply Now.

Controlling User Access to Remote Servers

Users can connect to a remote server by choosing the "Connect to Server" command in the Finder Go menu and providing the server's name or IP address. If you don't want users to access this menu item, you can hide the command.

To hide the "Connect to Server" command:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Finder, click Commands, and then set the management setting to Always.
5. Deselect "Connect to Server."
6. Click Apply Now.

Controlling User Access to an iDisk

If users want to connect to an iDisk, they can choose the "Go to iDisk" command in the Finder Go menu. If you don't want users to access this menu item, you can hide the command.

To hide the "Go to iDisk" command:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Commands, and then set the management setting to Always.

5 Deselect "Go to iDisk."

6 Click Apply Now.

Preventing Users from Ejecting Discs

If you don't want users to be able to eject discs (for example, CDs, DVDs, floppy disks, or FireWire drives), you can hide the Eject command in the Finder File menu.

To hide the Eject command:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Commands, and then set the management setting to Always.

5 Deselect Eject.

6 Click Apply Now.

Hiding the Burn Disc Command in the Finder

On computers with relevant hardware, users can burn discs (write information to recordable CDs or DVDs). If you don't want users to have this ability, you can hide the Burn Disc command in the Finder File menu.

To prevent users from using or burning recordable CDs or DVDs, use settings in the Media Access panes. For more information, see "Managing Media Access Preferences" on page 212.

Only computers with a CD-RW drive, Combo Drive, or SuperDrive can burn CDs. The Burn Disc command works only with CD-R, CD-RW, or DVD-R discs. Only a SuperDrive can burn DVD-R discs.

To hide the Burn Disc command:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Commands, and then set the management setting to Always.

5 Deselect "Burn Disc."

6 Click Apply Now.

Controlling User Access to Folders

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

To hide the "Go to Folder" command:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Commands, and then set the management setting to Always.

5 Deselect "Go to Folder."

6 Click Apply Now.

Removing Restart and Shut Down from the Apple Menu

If you don't want to allow users to restart or shut down the computer they're using, you can remove the Restart and Shut Down commands from the Apple menu.

To hide the Restart and Shut Down commands:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Commands, and then set the management setting to Always.

5 Deselect Restart and Shut Down.

6 Click Apply Now.

As an additional preventive measure, you can remove the Restart and Shut Down buttons from the login window by using settings in Login preferences. For instructions, see "Changing the Appearance of the Login Window" on page 201.

Adjusting the Appearance and Arrangement of Desktop Items

Items on a user's desktop appear as icons. You can control the size of desktop icons and how they're arranged.

To set preferences for the desktop view:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Views, and then select a management setting.

The management setting applies to options in all three views.

5 Click Desktop View and then drag the Icon Size slider to adjust the icon size.

6 To keep items aligned in rows and columns, select "Snap to grid."

7 To arrange items by criteria such as name or type (for example, all folders grouped together), select "Keep arranged by" and then choose a method from the pop-up menu.

8 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, as well as whether to show the toolbar in a Finder window.

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

To set preferences for Default and Computer Views:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Finder, click Views, and then set the management setting to Once or Always.

This setting applies to options in all three views.

5 Click Default View or Computer View.

Available settings are similar for both views.

6 Drag the Icon Size slider to adjust the icon size.

7 To keep icons aligned in rows and columns, select "Snap to grid."

Arranging icons in a grid prevents icons from overlapping.

8 To sort icons, select "Keep arranged by" and then choose a method from the 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.

If you select "Use relative dates," an item's creation or modification date appears as Today instead of 3/24/09.

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.

10 Select a size for icons in a list.

11 Click Apply Now.

Managing Login Preferences

Use Login preferences to set options for user login, to provide password hints, and to control the user's ability to restart and shut down the computer from the login window. You can also mount a group volume or set applications to open when a user logs in.

The table below summarizes what you can do with settings in each Login pane.

Login preference pane	What you can control
Window	*For computers and computer groups only:* The appearance of the login window such as the heading, message, which users are listed if the "List of users" is specified, and the ability to restart or shut down
Options	*For computers and computer groups only:* Login window options like enabling password hints, automatic login, console, fast user switching, inactivity log out, disabling of management, setting the computer name to match the computer record, and external account login
Access	*For computers and computer groups only:* Who can log in, if local users can use workgroup settings, and the combination and selection of workgroups
Scripts	*For computers and computer groups only:* Specify a script to run during login or logout and whether to execute or disable the client computer's LoginHook or LogoutHook scripts
Items	Access to the group volume, which applications open automatically for the user; and if users can add or remove login items

Scripts, Login Window, and Options can be managed for computers only, not for users or groups.

Changing the Appearance of the Login Window

You can easily change the appearance of a computer's login window. These settings include the login window's heading message, which users are listed and how, and the display of the restart and shut down buttons. These settings apply only to computers and computer groups.

When you display a list of users, you can choose which types of users to list. The effect of these settings depends on the version of Mac OS X installed on client computers.

List setting	Mac OS X version	Effect
Show local users	10.4	Lists local accounts and mobile accounts with a local home folder
Show local users	10.5 or later	Lists local accounts
Show mobile accounts	10.4	N/A
Show mobile accounts	10.5 or later	Lists mobile accounts with a local home folder and external accounts
Show network users	10.4 or later	Lists network accounts and mobile accounts without a local home folder
Show computer administrators	10.4 or later	Lists local system administrators
Show "Other..."	10.4 or later	Displays name and password text fields, allowing the user to authenticate with a local or network-based account

The directory administrator account is considered a network account, and is therefore hidden when you don't show network users. Another way to hide this account would be to set the directory administrator account's user ID to below 100. For more information, see "Modifying User IDs" on page 69.

You can customize the login window to suit your needs.

For example, to test a computer's ability to access the directory domain you could change the heading to Directory status and display a list of network users.

Or, to prevent unauthorized access, you could create a warning message, display the name and password fields (forcing intruders to know a user's name and password), and disable showing the Restart and Shut Down buttons (to help prevent intruders from bypassing the login window).

To change the appearance of the Login Window:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Login and then click Window.
5. Set the management setting to Always.
6. To change the default heading, choose a heading from the Heading pop-up menu.

   Users can view other headings by clicking the heading in the login window.
7. To display a message below the login window's heading, enter a message in Message.
8. To require the user to enter his or her user name and password, select "Name and password text fields."
9. To allow a user to select his or her name from a list, select "List of users able to use these computers."
10. Select categories of users you want to display in the list:
    - To ensure that a type of user doesn't show up in the list, deselect the corresponding setting.
    - To display mobile accounts on client computers with Mac OS X v10.5 or later, select "Show mobile accounts."
    - To display mobile accounts on client computers with Mac OS X v10.4 installed, select "Show local users."
    - To allow unlisted users to log in, select "Show Other."
11. To allow the user to restart the computer, select "Show Restart button."

    If the user has physical access to the computer, he or she can still restart the computer.
12. To allow the user to shut down the computer, select "Show Shut Down button."

    If the user has physical access to the computer, he or she can still shut down the computer.

    You might also want to remove the Restart and Shut Down commands from the Finder. For more information, see "Managing Finder Preferences" on page 193.
13. Click Apply Now.

Configuring Miscellaneous Login Options

You can configure the following login options that don't change the appearance of the login window but affect how users log in.

Option	What this does when enabled
Show password hint when needed and available	If the user supplied a password hint and he or she enters an incorrect password three times, the password hint appears.
Enable automatic login	If the computer's local settings enable Automatic Login, the login window is bypassed when the computer starts up.
Enable >console login	Users can log in using the Darwin console (command-line interface). To log in to the console, the user enters ">console" and no password in the login window. This allows the user to bypass management.
Enable Fast User Switching	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, allowing you to switch to a different account by choosing it. A user must authenticate to switch to his or her account, but the previous user does not need to log out first.
Log out users after # minutes of activity	If a client computer has Mac OS X v10.4 or later, when the set time interval has passed, the user is logged out and returned to the login window.
Local administrators may refresh or disable management	When local administrators log in, they have the option not to choose a workgroup and to disable preference management.

Option	What this does when enabled
Set computer name to computer record name	*For computers with Mac OS X v10.5 or later:* You can set the computer name. This name affects the client computer's Bonjour name, which other computers on the local subnet use to access the client computer. The new Bonjour name is *name-#*.local where *name* is the computer record name you specify and # uniquely identifies the computer if there are several computers with the same Bonjour name.
Enable external accounts	*For computers with Mac OS X v10.5 or later:* Users can log in using external accounts. If the login window displays a list of user names, the external account is listed as a mobile account. If the login window displays a name and password field, the user must enter the external account name and password.
Enable guest account	*For computers with Mac OS X v10.5 or later:* Users can log in using the guest account. The guest account allows anyone to access the computer without requiring a password. To manage guest users, manage the computers or computer groups with enabled guest accounts.

To configure miscellaneous login options:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Login and then click Options.
5. Set the management setting to Always.
6. Select the options you want to enable and click Apply Now.

Choosing Who Can Log In

Workgroup Manager gives you control over who is allowed to access computers. You can choose which network users are allowed to log in and whether local users can log in.

Denying access supersedes allowing access. If you allow computer access to a group of network users, you can deny access to specific members of the group. However, if you deny computer access to a group, you can't allow computer access to specific members of that group.

If you don't list users or groups to allow or deny access to, all network users can log in. If you add users or groups to the list, only users and groups that are explicitly allowed access can log in.

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

To choose who can log in:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Login, click Access, and then set the management setting to Always.
5. To control access for all network users, click the Add Network Users (gear) button.

   If you allow access for the Network Users group, you can prevent access for specific users or groups. All other network users and groups are allowed access.

   If you deny access for the Network Users group, all network users and groups are denied access even if they are specifically allowed access in the list.
6. To control access for specific users or groups, click the Add (+) button and then drag user or group accounts from the drawer to the list.

   To switch the drawer's display of user accounts to group accounts or vice-versa, click the Users or Groups button at the top of the drawer.
7. To allow or deny access to a user or group in the Access Control List, choose Allow or Deny from the Access pop-up menu for that user or group.
8. To allow local users to access the computer, select "Local-only users may login."
9. Click Apply Now.

Customizing the Workgroups Displayed at Login

You can change settings that affect how workgroup preferences and other settings impact a user's experience. For example, you can require local users to choose a workgroup.

This makes the user's environment the same as if he or she was a member of the workgroup. Or, you can configure how to handle situations where multiple workgroups are available for a user.

The following access options control workgroup settings at login.

Option	What this does when enabled
Local-only users use available workgroup settings	*For computers with Mac OS X v10.4 or later:* Local users must choose a workgroup when logging in. The user can choose from all workgroups that can access the computer. The user's environment is the same as if he or she was a member of the workgroup.
Ignore workgroup nesting	*For computers with Mac OS X v10.5 or later:* The user can choose whether to use managed preferences from a parent group or its child group. Only the preferences of the chosen group apply. When disabled, the preferences of parent and child groups apply.
Combine available workgroup settings	*For computers with Mac OS X v10.5 or later:* The user's preferences are based on the combination of preferences from all user's workgroups. For local users, all workgroups that can access the computer are combined. When enabled, the user can't select the workgroup to use. When disabled, the user can select which workgroup to use. If the user selects a parent or child group, the preferences of both apply.
Always show workgroup dialog during login	*For computers with Mac OS X v10.5 or later:* The dialog displaying all available workgroups appears even when there are no workgroups available.

To customize the workgroups displayed at login:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Login, click Access, and then set the management setting to Always.
5. Select the workgroup settings to enable them.
6. When you finish enabling workgroup settings, click Apply Now.

To view the workgroup a user selects at login:

1 Connect to the client computer using an account with administrator privileges.

```
$ ssh admin@computer.name
```

Replace *admin* with the short name of the client computer's administrator and *computer.name* with the IP address or the DNS name of the client computer.

2 Convert the binary com.apple.MCX.plist file to XML format.

```
$ sudo plutil -convert xml1 /Library/Managed\ Preferences/shortname/com.
    apple.MCX.plist
```

Replace *shortname* with the short name of the logged-in client account.

3 View the workgroup key in /Library/Managed Preferences/shortname/com.apple.MCX.plist file.

```
$ cat /Library/Managed\ Preferences/shortname/com.apple.MCX.plist
```

Replace *shortname* with the short name of the logged-in client account.

Enabling the Use of Login and Logout Scripts

You can use login scripts to perform a set of actions when a user logs in or logs out.

Because login or logout scripts run as root, they are very powerful. Test your scripts to make sure they don't negatively impact system settings or damage user files.

You can add a login script to a computer in two ways:

- Add a LoginHook script to a specific computer
- Apply a login script to a computer or computer group using Workgroup Manager

When enabling the use of login and logout scripts, you can set a trust value for the client. Trust values determine the required level of authentication before a client trusts a server enough to run its scripts. Most trust values directly correlate to LDAP security policy settings that are configured in Directory Utility.

The trust value of DHCP doesn't correlate to a security policy. Instead, it correlates to whether Directory Utility is configured to use a DHCP-supplied LDAP server. The trust value of Authenticated requires that you set up trusted binding to an LDAP directory.

For more information about how to use Directory Utility to enable LDAP security policies using DHCP-supplied LDAP, or for setting up trusted binding, see *Open Directory Administration*.

The following table lists trust values and requirements. The table is arranged in order of increasing trust, where the last entry requires the highest level of trust.

Trust value name	Requirements
Anonymous	None. The client trusts any directory domain server.
DHCP	In Directory Utility, select "Add DHCP-supplied LDAP servers to automatic search policies."
Encryption	In Directory Utility, select "Encrypt all packets (requires SSL or Kerberos)."
Authenticated	Set up trusted binding between the client computer and the LDAP directory.
PartialTrust	In Directory Utility, select "Digitally sign all packets (requires Kerberos)." Most Active Directory nodes support PartialTrust but not FullTrust.
FullTrust	In Directory Utility, select "Block man-in-the-middle attacks (requires Kerberos)" and "Digitally sign all packets (requires Kerberos)."

To set the minimum required trust level, set the MCXScriptTrust client setting:

- If the client's MCXScriptTrust setting is a level of trust equal to or less than the trust value, the client trusts the server and runs its login and logout scripts.
- If the client's MCXScriptTrust setting is a level of trust more than the trust value, the client doesn't trust the server and doesn't run its scripts.

The default trust value is FullTrust.

To enable the use of login or logout scripts:

1. Log in to the user's computer locally or use Apple Remote Desktop.
2. Open the Sharing pane of System Preferences.
3. Click the lock to authenticate, and enter the name of a local or directory administrator.
4. Click Edit.
5. If the local host name contains special nonalphabetic or nonnumeric characters such as spaces, dashes, and underscores, remove the special characters and then click OK.

   For example, change local host names like "Anne-Johnson's-Computer" to "AnneJohnsonsComputer."
6. Optionally, determine the trust level by entering the following command in Terminal:

```
dscl localhost -read /LDAPv3/www.apple.com dsAttrTypeStandard:TrustInform
    ation
```

Replace `www.apple.com` with the address of your LDAP directory. Running this command displays a line similar to the following:

```
TrustInformation: Authenticated FullTrust
```

In this example, the current trust level is FullTrust. The trust level is also Authenticated. When two trust levels are listed, the higher trust level takes precedence.

7 Set the "EnableMCXLoginScripts" key in ~root/Library/Preferences/com.apple.loginwindow.plist to TRUE by entering the following command in Terminal:

```
sudo defaults write com.apple.loginwindow EnableMCXLoginScripts -bool
     TRUE
```

8 To change the trust value from FullTrust, set the "MCXScriptTrust" key in ~root/Library/Preferences/com.apple.loginwindow.plist to a valid trust value.

For example, enter the following command in Terminal:

```
sudo defaults write com.apple.loginwindow MCXScriptTrust -string
     PartialTrust
```

This command sets the trust value to PartialTrust. To set other trust values, replace PartialTrust with other trust values. If you enter an invalid trust value, the trust value is reset to FullTrust.

When you enable login and logout scripts or change the trust value, add login and logout scripts in Workgroup Manager. For more information about how to use Workgroup Manager to add login and logout scripts, see "Choosing a Login or Logout Script."

Choosing a Login or Logout Script

You can only run login and logout scripts on computers or computer groups. Before adding scripts, you must enable them using login and logout scripts. If you change the trust level for client computers running Mac OS X v10.4, re-add your scripts.

For instructions on enabling login and logout scripts on clients and for more information about trust levels, see "Enabling the Use of Login and Logout Scripts" on page 207.

If you run login or logout scripts for computers and computer groups, the script for the computer is run first, followed by the script for the computer group, starting with hierarchical groups and ending with parent groups.

You can't run scripts that are larger than 30 KB.

To choose login or logout scripts:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3 Select one or more computers or computer groups.

4 Click Login and then click Scripts.

5 Set the management setting to Always.

6 Select Login Script or Log-Out Script, then in the dialog that appears, locate your script and click Open.

7 Click Apply Now.

Automatically Opening Items After a User Logs In

You can simplify the user experience by setting frequently used items such as applications, folders, or server connections to open when the user logs in. You can also hide the items to help prevent screen clutter while still making the items easily accessible.

Items open in the order they appear in Login Items preferences. You specify the order. The last item opened becomes the active application. For example, if you specify three items to open (and none are hidden), the user sees the menu bar for the last item opened. If an application has open windows, the windows might 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 set an item to open automatically:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Login and then click Items.

5 Select a management setting.

6 To add an item to the list, click the Add (+) button, select the application, folder, or server you want to automatically open, and then click Add.

7 For any item you don't want the user to see right away, select its Hide checkbox.

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 To automatically connect the user to a server, select the server and then select "Authenticate selected share point with user's login name and password."

The server must use the same directory domain as the one the user logs in to.

9 If you don't want users to have the ability to add and remove items, deselect "User may add and remove additional items."

This option is available only if Login Items preferences are always managed. If you only manage Login Items preferences Once, a user can remove any items added to the login list.

Users can't remove items added to the login items list but they can remove items they've added themselves.

10 To prevent users from stopping applications that open automatically at login, deselect "User may press Shift to keep items from opening."

This option is available only if Login Items preferences are always managed.

11 If you select Once, you can click "Merge with user's items."

This produces two results, depending on whether the user has items in their login list.

If the user has items listed in their login list, either by the user adding them or by having items previously added through preference management, merging only opens login items that appear on the user's list and on your list.

If the user's login list does not include items, all managed login items appear.

If you do not select "Merge with user's items," all login items on either list open.

12 Click Apply Now.

Providing Access to a User's Network Home Folder

Don't provide access to a user's network home folder to users with mobile accounts on Mac OS X v10.4 or later. Mac OS X v10.4 and later include portable home directories, which provide a synced subset of the user's local and network home folders.

If a user modifies files in the local and network home folders, when the two home folders sync, the newer modifications take precedence, which could surprise and confuse the user. Additionally, users could be confused by having multiple folders titled with their user names and similarly named folders like Documents, Music, and others.

To automatically mount the Network Home:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3 Select a mobile user account in the account list.

4 Click Login and then click Items.

5 Select a management setting.

6 Select "Add network home share point."

7 Click Apply Now.

Providing Easy Access to the Group Share Point

After you set up a group share point, you can make it easy for users to locate group folders by automatically connecting to the share point at login.

The connection to the group share point uses the user name and password given at login.

When you manage Finder preferences, you can choose to not show connected servers, which removes the group volume icon from the desktop.

If you change the location of the group share point, update the login item for the group in Workgroup Manager.

For information about setting up a group share point, see "Creating a Group Folder" on page 111.

Note: This preference setting applies only to groups. You can't 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.
2. In Workgroup Manager, click Preferences.
3. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
4. Click the Groups button and select one or more group accounts from the list.
5. Click Login and then click Items.
6. Set the management setting to Always.
7. Select "Add group share point."
8. Select the newly added group share point item.

   If you don't want the group share point to appear in the Dock, select the Hide checkbox.
9. Make sure "Mount share point with user's name and password" is selected.
10. Click Apply Now.

Managing Media Access Preferences

Media Access preferences let you control settings for and access to CDs, DVDs, the local hard disk, and external disks (for example, floppy disks and FireWire drives).

The table below describes what you can do with the settings in each Media Access pane.

Media Access preference pane	What you can control
Disc Media	Settings for CDs, DVDs, and recordable discs (for example, CD-R,CD-RW, or DVD-R). Computers without relevant hardware are not affected by these settings.
Other Media	Internal hard disks and external disks (other than CDs or DVDs).

Controlling Access to CDs, DVDs, and Recordable Discs

You can control whether users can play or record CDs or DVDs. However, you can't deny access to specific discs or to specific items on a disc.

If a computer has a recordable disc drive, you can control a user's ability to burn discs—that is, to write information on a recordable disc such as a CD-R, CD-RW, or DVD-R. Users can burn CDs on computers with a CD-RW drive, Combo Drive, or SuperDrive. Users can burn DVDs only on computers with a SuperDrive.

To control access to disc media:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Media Access and then set the management setting to Always.

   This setting applies to all Media Access preference options.
5. Click Disc Media and select the desired options.

   If you select Require Authentication, the user must authenticate as a local administrator to use the disc media.

   Before you can select Require Authentication, you must first select Allow.
6. Click Apply Now.

Controlling Access to Hard Drives, Disks, and Disk Images

You can control access to internal or external disk drives such as floppy disk drives, Zip drives, USB drives, and FireWire drives. You can also control access to disk images (files with the .dmg extension). If your managed computers use Mac OS X v10.6 or later, you can control access to DVD-RAM discs.

If you disallow external disks, external disks do not appear in the Finder. If you disallow disk images, the images are visible in the Finder but users can't open them.

To restrict access to internal and external disks:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
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 Require Authentication, the user must authenticate as a local administrator to use the disc media.

   If you select Read-Only, users can view the contents of a disk but can't change it or save files on it.

   Before you can select Require Authentication or Read-Only, you must select Allow.
7. Click Apply Now.

Ejecting Removable Media Automatically When a User Logs Out

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

To automatically eject removable media:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Media Access.
5. Set the management setting to Always.

   This setting applies to all Media Access preference options.
6. In Disc Media or Other Media, select "Eject all removable media at logout."
7. Click Apply Now.

Managing Mobility Preferences

You can automatically create mobile accounts for users during their next login.

If your computers use Mac OS X v10.5 or later, you can also encrypt the contents of the mobile account's portable home directory, restrict its size, choose its location, or set an expiration date on the account.

The table below describes what you can do with the settings in each Mobility pane.

Mobility preference pane	What you can control
Account Creation	Whether to create mobile accounts when users log in and whether to encrypt contents of the portable home directory, restrict its size, or choose a different location for it
Account Expiry	Whether to delete mobile accounts and how soon to do so after the user's next login
Rules	The folders you want to sync at login and logout (or in the background) and how frequently to sync folders in the background

For planning information and other considerations for mobile accounts, see Chapter 8, "Managing Portable Computers."

Creating a Mobile Account

You can use Workgroup Manager to create a mobile account when a user logs in. If you don't enable the creation of mobile accounts, the user logs in using a network account. When you enable mobile accounts, a local home folder is created for the user at first login.

When the user's local home folder is created, it's based on a template stored on the local computer. The user's network home folder is based on a template stored on the server hosting home folders.

When you modify these templates, you change the user's default home folder structure and content, and you can modify the ~/Library folder, allowing you to set default bookmarks and application preferences.

You can choose whether local and network home folders initially sync, in which case the network home folder replaces the local home folder.

You must authenticate as root to change the template stored in /System/Library/User Template/*language*.lproj. Replace *language* with the language used on the client computer, such as English.

Note: When a mobile account is enabled, it appears in the login window and in the Accounts pane of System Preferences with the label *Mobile*. When the account is selected in the Accounts pane, some settings might appear dimmed.

To create a mobile account using Workgroup Manager:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select a user account, group account, computer, or computer group.

   When users log in to a workgroup with mobile-account creation enabled, they are given individual mobile accounts. Similarly, if you enable mobile accounts for a computer or a computer group, when users log in using the computer or a computer in the computer group, users are given individual mobile accounts for that computer.
4. Click Mobility, click Account Creation, and then click Creation.
5. Set the management setting to Always.
6. Select "Create mobile account when user logs in to network account."
7. If you want the user to decide whether to enable a mobile account at login, select "Require confirmation before creating mobile account."

   If this option is selected, the user sees a confirmation when logging in. The user can click Create Now to create a local home folder and enable the mobile account, click Don't Create to log in as a network user without enabling the mobile account, or click Cancel Login to return to the login window.

   If you select "Show 'Don't ask me again' checkbox," the dialog allows the user to prevent the display of the dialog on that computer. If the user selects "Don't ask me again" and then clicks "Don't Create," he or she isn't asked to create a mobile account on that computer. The user can hold down the Option key during login to redisplay the dialog.
8. To initially sync local and network homes so that the network home folder replaces the local home folder, select "Create home using network home and default sync settings." To create the local home folder using the local home template, select "Create home using local home template."

   If you sync the local and network homes folders, the default Mac OS X sync settings (those in the Accounts pane of System Preferences) are enabled. If you create the local home folder using the local home template, the default Mac OS X sync settings are disabled. In both cases, managed sync settings apply.
9. Click Apply Now.

   Changes are applied to a mobile account the next time the computer connects to the network.

Preventing the Creation of a Mobile Account

To prevent the creation of mobile accounts, manage Mobility preferences.

After a user creates a mobile account, the local home folder for that account stays on the computer until it's deleted. You can delete local home folders to save disk space, or you can set an expiration period on the mobile account so local home folders are deleted when the account expires.

For instructions, see "Manually Removing Mobile Accounts from Computers" on page 217, and "Setting Expiration Periods for Mobile Accounts" on page 223.

To prevent the creation of mobile accounts:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility, click Account Creation, and then click Creation.
5. Set the management setting to Always.
6. Deselect "Create mobile account when user logs in to network account."
7. Click Apply Now.

Manually Removing Mobile Accounts from Computers

If a user no longer requires a mobile account, you can delete the account. When you delete the account, you can also delete or archive the user's local home folder.

To delete a mobile account, you must log in to the computer using an account other than the mobile account. You must also know the name and password of an administrator account on the computer.

If you want to use Workgroup Manager to remove the mobile account remotely, you can set a null expiration period for the account. By doing so, you remove the mobile account from all computers. For more information, see "Setting Expiration Periods for Mobile Accounts" on page 223.

To remove a mobile account:

1. On the client computer, log in using a different account from the one you're removing the mobile account of.
2. Open System Preferences.
3. Click Accounts and then click the lock and authenticate as the local administrator.
4. To list all accounts, click the Other Accounts disclosure triangle and then select the mobile account you want to remove.

   The mobile account should have the word "Mobile" listed.
5. Click the Delete (–) button.

6 Choose one of the following home folder options and then click OK.

Option	Effect
Save the home folder in a disk image	Removes a user account from the local directory domain but preserves the local home folder in /Users/*username*.dmg, where *username* is the short name of the deleted user.
Do not change the home folder	Removes a user account from the local directory domain but preserves the local home folder in /Users as "*username* (Deleted)," where *username* is the short name of the deleted user.
Delete the home folder	Removes a user account from the local directory domain and permanently deletes the user's home folders.

Enabling FileVault for Mobile Accounts

If your users have computers with Mac OS X v10.5 or later installed, you can use FileVault to encrypt the local home folders for their mobile accounts.

FileVault encrypts the user's local home folder using the Advanced Encryption Standard with 128-bit keys (AES-128). The home folder content is safe even if the user's computer is stolen or if an intruder attempts to use the computer while the user is not logged in.

The user's login password is used to decrypt and give the user access to his or her FileVault-protected account. If the user forgets the login password and a computer administrator has set a master password, the administrator can use the master password to unlock all local accounts.

You can choose whether to require master passwords when enabling FileVault protection for mobile accounts:

- If you don't require a master password and there is no master password, local computer administrators can't unlock the account.
- If you require a master password and there is no master password, the user can't enable a mobile account.
- If you select "Require confirmation before creating mobile account," the user can log in with a network account. Network accounts don't have local home folders (preventing intruders from accessing home folder content).

If you enable FileVault, you can restrict the size of the local home folder. When you set a network home disk quota (in the Home pane of a user account), it limits the amount of space available for the user's network home folder.

By restricting the size of the local home folder, you prevent the user's local home folder from using more space than is available in the user's network home folder. This ensures that the home folders can sync without requiring more space than is available in the network home folder.

Additionally, if you make the maximum size of the local home folder smaller than the network home disk quota, you can provide more flexibility for handling files with sync conflicts.

If a mobile account is protected with FileVault, the user must be logged in to share files using File Sharing.

To enable FileVault for mobile accounts:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility, click Account Creation, and then click Creation.
5. Set the management setting to Always.
6. Select "Create mobile account when user logs in to network account."

   You must select this option to enable a mobile account for the selected account.
7. To allow the user to choose *not* to create a local home folder (so that instead of a mobile account, the user logs in with a network account), select "Require confirmation before creating mobile account."

   If you require a master password but the user logs in to computers without master passwords set, selecting this allows the user to log in with a network account.
8. Click Options.
9. Select "Encrypt contents with FileVault," then select "Use master password, if available" or "Require computer master password."

   If you select "Use master password, if available," the mobile account uses FileVault regardless of whether there is a master password already set.

   If you select "Require computer master password" and there is no master password set, the user might be able to log in with a network account, depending on whether you selected "Require confirmation before creating mobile account" in the Creation pane.
10. To restrict the size of the local home folder, select "Restrict size" and select "to fixed size" or "to percentage of network home quota"; then enter a value that is less than the size of your network home folder's disk quota.

    If you didn't set a disk quota, select "to fixed size."

For more information about setting a disk quota, see "Creating a Network Home Folder" on page 133.

11 Click Apply Now.

Selecting the Location of a Mobile Account

You can select the location of a mobile account's local home folder or you can let the user select the location. If you select the location, choose from one of the following.

Home folder location	Description
on startup volume	The local home folder is located on the startup volume in /Users/. This is the default location where the local home folders of mobile accounts on computers with Mac OS X v10.4 and earlier are stored.
at path	The local home folder is located at the path you specify. You can specify a different volume by entering /Volumes/*DriveName/Folder/*, where *DriveName* is the name of the volume, and *Folder* is the folder in the volume. If you don't specify a volume, the location is on the startup volume.
user chooses	When users with mobile accounts log in, a window appears that allows them to choose a location for the local home folder. After they choose a location, the window only appears when a mobile account is being created. You can choose which types of volumes the user is allowed to choose from: • "any volume" includes volumes on internal or external hard disks • "any internal volume" includes volumes on internal hard disks • "any external volume" includes volumes on external hard disks

If you choose a location at a specific path, make sure the folder has the following permissions.

Type	Name	Privilege
Owner	system	Read & Write
Group	admin	Read only
Others	Others	Read only

If you choose a location that doesn't exist on the user's computer, it is created when the user logs in.

When a location is chosen on an external disk, you create an external account. For more information, see "Creating External Accounts" on page 221.

To select the location of a mobile account:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility, click Account Creation, click Creation, and then set the management setting to Always.
5. Select "Create mobile account when user logs in to network account."

   You must select this option to enable a mobile account for the selected account.
6. Click Options and then set the management setting to Always.
7. Select a "Home folder location" option.

   If you select "at path," enter the path to a folder on an external drive in the format /Volumes/*DriveName/Folder*, replacing *DriveName* with the name of the external drive and *Folder* with a folder on the external drive. If you don't specify a volume, the location is on the startup volume.

   If you select "user chooses," choose a type of volume from the pop-up menu to allow the user to store his or her local home folder on that type of volume.
8. Click Apply Now.

Creating External Accounts

An external account is a mobile account where the local home folder is stored on an external drive, allowing the user to access his or her account on any computer with Mac OS X v10.5 or later.

The user's local home folder is stored entirely on the external drive and leaves no remnants on computers. External accounts also save hard disk space on the computer, which is especially important if you don't set an account expiration or if many users create mobile accounts with local home folders on the same computer.

To determine the location of the external account, choose from the following. All of these ways can be used to set up external accounts:

- If you set the location to "on startup volume," the mobile account doesn't immediately become an external account. After creating the local home folder, if the user starts target disk mode on the computer and connects it to a client computer, the mobile account then becomes an external account.
- If you set the location to "at path," you can enter the path for the mobile account's local home folder. If you enter a path for an external drive, a local home folder is created on the external drive after the user logs in.
- If you set the location to "user chooses volume," when the user logs in, a window appears allowing the user to choose whether to store the local home folder on the computer or on an external drive. If the user chooses an external drive, a local home folder is created on the external drive.

To create an external account:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility, click Account Creation, click Creation, and then set the management setting to Always.
5. Select "Create mobile account when user logs in to network account."

   You must select this option to enable a mobile account for the selected account.
6. Click Options and then set the management setting to Always.
7. For the home folder location, select "at path," "user selects volume," or "any volume:"
   - If you select "at path," enter the path to a folder on an external drive in the format /Volumes/*DriveName/Folders*, replacing *DriveName* with the name of the external drive and *Folders* with a folder on the external drive.
   - If you select "user selects volume," choose "any external volume" or "any volume" from the pop-up menu. After authenticating at the login window, the user is prompted to choose a location.
   - If you select "any volume", the user can choose either on the local hard disk or on the external hard disk. If the user chooses the external hard disk, the local home folder is stored in /Users/*ShortName*, where *ShortName* is the user's short name.
8. Click Apply Now.

Setting Expiration Periods for Mobile Accounts

When a user enables a mobile account, Mac OS X usually creates a local home folder on the computer he or she is using. If that user enables mobile accounts on several computers, each of those computers has a local home folder for the user. If the user doesn't use those computers, the local home folders are unused and waste disk space.

When you set an expiration period on a mobile account, the mobile account and its local home folder are deleted after a period of inactivity.

You can also set an expiration period of 0 to delete the mobile account and its local home folder as soon as possible. Depending on the account type you're managing, "as soon as possible" refers to one of these events:

- For users and groups, the mobile account and its local home folder are deleted after the user logs out.
- For computers and computer groups, the mobile account and its local home folder are deleted the next time the login window appears. This doesn't include when the login window appears while using fast user switching.

Expiry settings do not affect external accounts.

To set an expiration period:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility and then click Account Expiry.
5. Set the management setting to Always.
6. Select "Delete mobile accounts" and enter a number of hours, days, or weeks.
7. To wait until after the user's mobile account syncs to delete the local home folder, select "Delete only after successful sync."
8. Click Apply Now.

Choosing Folders to Sync

You can use Workgroup Manager to choose which folders to sync at login, logout, in the background, or manually for users with mobile accounts. You can also choose not to sync specific folders.

There are two types of syncs: *preference sync* and *home sync*. Preference sync is used for preference files, which are typically stored in ~/Library. Home sync is used for files in the user's home folder (~) but not ~/Library.

The two syncs differ in how they handle conflict resolution and background syncing.

- Sync conflicts occur when a file changes on the client and the server since the last sync. For preference syncing, if you have login and logout sync enabled, when users log in, network files override conflicting client files, but when users log out, client files override conflicting network files. When files don't conflict, newer files override older files regardless of if they're on the server or the client.
- When a preference sync occurs in the background, preference files sync from the client to the server but not from the server to the client. If preference files on the server are newer than preference files on the client, the sync can only complete at login or logout.

Be careful with login and logout syncing. A user's login and logout is delayed while files are syncing. Using background syncing can also cause users to load outdated files from the network, especially when syncing is set to occur at long intervals.

For considerations when choosing folders to sync and how to sync them, see "Strategies for Syncing Content" on page 150.

To choose folders to sync:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select users, groups, computers, or computer groups.
4. Click Mobility, click Rules, and then click Preference Sync or Home Sync.
5. Select a management setting.
6. Select "Sync at login," "Sync at logout," "Sync in the background," or "Sync manually."
7. Add folders by doing one of the following:
   - Click Add (+) for the Sync lists and enter the path to the folder you want to sync.

     Precede the folder with ~/ to specify the location of the synced folder in the user's home folder. For example, to sync the user's Documents folder, enter ~/Documents.
   - Click Browse (...) for the Sync lists to browse to a folder.

     Because you are browsing the computer running Workgroup Manager, you might choose a folder that is not located in the user's account. If you choose a folder that doesn't exist in the user's account, no files are synced.
8. To choose *not* to sync files or folders, use Add (+) or Browse (...) buttons to add items to the "Skip items that match any of the following" list.

   To filter for specific items, click the Match field entry for any list item.

9 To add synced folders to folders the user selects for syncing, select "Merge with user's settings."

If you sync the same folder in Workgroup Manager as the user chooses in the Accounts pane of System Preferences, merging causes the Workgroup Manager sync settings to take precedence. If you do not select "Merge with user's settings," the folders you sync replace those chosen by the user.

When used with the Once setting, merging with the user's settings is useful for adding folders without disrupting the folders the user has set to sync.

10 Click Apply Now.

Stopping Files from Syncing for a Mobile Account

To stop a mobile account from syncing files, you must manage its login and logout and background sync rules. If you leave them unmanaged, the user's current sync settings remain in effect and the user can choose his or her sync settings in the Accounts pane of System Preferences.

To stop files from syncing:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Mobility and then click Rules.

5 Click Login & Logout Sync and then set the management setting to Always.

6 Deselect "Sync at login and logout."

7 Click Background Sync and then set the management setting to Always.

8 Deselect "Sync in the background."

9 Click Apply Now.

Setting the Background Sync Frequency

You can change the frequency of syncing for background folders. By default, background folders sync every 20 minutes. You can set frequencies from 5 minutes to 8 hours.

If you set the frequency to a long interval, you run a higher risk of users loading older, outdated files. If users save files and log off before the background files sync, when they load the same file on another computer, they might get either an older synced file or no file at all.

To set the frequency for syncing background folders:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Mobility, click Rules, and then click Background Sync.

   Make sure to select Once or Always and that there are items configured to sync in the background.
5. Click Options and then set the management setting to Always.
6. Click Every and drag the slider to set the frequency for background folder sync.

   If you want background folders to sync only when users choose to sync, click Manually.

   The default frequency is 20 minutes. The frequency you set also affects folders that users configure to sync automatically.
7. Click Apply Now.

Showing Mobile Account Status in the User's Menu Bar

If mobile account users run Mac OS X v10.5 or later, you can add a mobile account status menu to their menu bar. This status menu allows the user to do the following:

- View when he or she last synced
- Initiate a sync
- Change their home sync preferences

Home sync preferences correspond to Mobility preferences in Workgroup Manager. If you manage any Mobility preferences, users can't change those preferences.

Home sync preferences includes the following settings:

- Setting the home folder location
- Enabling FileVault
- Enabling background, login, and logout sync
- Selecting what is synced
- Setting the sync frequency
- Enabling the mobile account status menu

If you disable the mobile account status menu, the user can still configure his or her mobile account in the Accounts pane of System Preferences.

To show mobile account status in the user's menu bar:

1. In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Mobility, click Rules, and then click Options.

5 Set the management setting to Always.

6 Select "Show status in menu bar."

7 Click Apply Now.

Managing Network Preferences

Use Network preferences to select and configure proxy servers that can be used by users and groups. You can bypass proxy settings for specific hosts and domains. This has the advantage of providing a customized browsing experience for managed users and groups.

You can also disable Internet Sharing, AirPort, or Bluetooth. Disabling these can improve security by removing avenues for attack.

The table below describes what settings in each Network pane can do.

Network preference pane	What you can control
Proxies	Access to proxy servers, the ability to bypass proxy settings, and use of passive FTP mode
Sharing & Interfaces	Availability of Internet Sharing from the computer, and use of AirPort or Bluetooth

Configuring Proxy Servers by Port

You can configure specific types of proxies for a user or group to access and specify the port. The types of proxy servers that are individually modifiable are FTP, Web (HTTP), Secure Web (HTTPS), Streaming (RTSP), SOCKS, Gopher, and Automatic Proxy Configuration.

You must assign a single server for every type of proxy server (for example, you can't have multiple FTP proxy servers).

To configure proxy servers for a user or a group:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Network and then click Proxies.

5 Set the management setting to Always.

6 Select the specific type of proxy you want to configure (FTP, Web, and so on).

7 Specify a URL and a port using the form proxyserver.apple.com:8080.

8 Click Apply Now.

Allowing Users to Bypass Proxy Servers for Specific Domains

When managing Network preferences for users, you can allow them to bypass proxy settings for specific hosts or domains. Bypassing the proxy server lets users connect directly to specified addresses.

You must set up a proxy server before you can bypass it. For instructions, see "Configuring Proxy Servers by Port" on page 227.

To choose the domains that users can access directly:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Network and then click Proxies.

5 Set the management setting to Always.

6 In the "Bypass proxy settings for these Hosts & Domains" field, enter the addresses of the hosts and domains that you want users to be able to connect to directly.

To enter multiple address, separate the subnet masks with new lines, spaces, semicolons, or commas.

There are several ways to enter addresses:

- A subdomain or fully qualified domain name (FQDN) of a target server, such as server1.apple.com or store.apple.com.
- The specific IP address of a server, such as 192.168.2.1.
- A domain name, such as apple.com. This bypasses apple.com but not subdomains such as store.apple.com.
- An entire website including all subdomains, such as *.apple.com.
- A subnet in Classless Inter-Domain Routing (CIDR) notation. For example, to add a subnet of 192.168.2.x, you would name that view 192.168.2.0/24. For a detailed description of subnet masks and CIDR notation, see *Network Services Administration*.

7 Click Apply Now.

Enabling Passive FTP Mode

When managing Network preferences, you can require passive FTP mode. Passive FTP mode causes the FTP server to open a connection to the computer on a dynamically determined port. This can be more convenient for computers but it requires port filters to be properly configured on the FTP server.

To enable passive FTP mode:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Network and then click Proxies.
5. Set the management setting to Always.
6. Select Use Passive FTP Mode (PASV).
7. Click Apply Now.

Disabling Internet Sharing

Although Internet Sharing is a convenient way for computers to share Internet access, turning it on can disrupt your network (because it can cause conflicts with DHCP and NAT services).

To reenable Internet Sharing, you must log in to the computer locally and enable it in the Sharing pane of System Preferences.

To disable Internet Sharing:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Network and then click Sharing & Interfaces.
5. Set the management setting to Always.
6. Select Disable Internet Sharing.
7. Click Apply Now.

Disabling AirPort

If you disable AirPort, it is disabled the next time a computer retrieves managed preferences. If the computer had active AirPort connections, they are immediately disconnected.

To reenable AirPort, you must log in to the computer locally and enable it in the Network pane of System Preferences.

To disable AirPort:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Network and then click Sharing & Interfaces.
5. Set the management setting to Always.
6. Select Disable AirPort.
7. Click Apply Now.

Disabling Bluetooth

Before disabling Bluetooth, make sure your computers don't rely on Bluetooth-enabled input devices like keyboards and mice.

To reenable Bluetooth, you must log in to the computer locally and enable it in the Network pane of System Preferences.

To disable Bluetooth:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Network and then click Sharing & Interfaces.
5. Set the management setting to Always.
6. Select Disable Bluetooth.
7. Click Apply Now.

Managing Parental Controls Preferences

Parental Controls preferences allow you to hide profanity in Dictionary, limit access to websites, or set time limits or other contraints on computer usage. To manage Parental Controls preferences, computers must have Mac OS X v10.5 or later.

The table below describes what settings in each Parental Controls pane can do.

Parental Controls preference pane	What you can control
Content Filtering	Whether profanity is allowed in Dictionary, and limitations on which websites users can view
Time Limits	How long and when users can log in to their accounts

Hiding Profanity in Dictionary

You can hide profane terms from the Dictionary application included with Mac OS X v10.5 or later. When you hide profane terms, entirely profane terms are removed from search results. If you search for a profane term that has an alternate nonprofane definition, Dictionary only displays the nonprofane definition.

To hide profanity in Dictionary:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Parental Controls and then click Content Filtering.
5. Set the management setting to Always.
6. Select "Hide profanity in Dictionary."
7. Click Apply Now.

Preventing Access to Adult Websites

You can use Workgroup Manager to help prevent users from visiting adult websites. You can also block access to specific websites while allowing users to access other websites. You can allow or deny access to specific subfolders in the same website.

Instead of preventing access to specific websites, you can allow access only to specific websites. For more information, see "Allowing Access Only to Specific Websites" on page 232.

To prevent access to specific websites:

1. In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Parental Controls and then click Content Filtering.

5 Set the management setting to Always.

6 Select "Limit access to websites by" and choose "trying to limit access to adult websites."

7 To allow access to specific sites, click the Add (+) button next to the "Always allow sites at these URLs" list and then enter the URL of the site you want to allow.

8 To block access to specific sites, click the Add (+) button next to the "Never allow sites at these URLs" list and then enter the URL of the site you want to block.

To allow or block a site, including all content stored in its subfolders, enter the highest level URL of the site.

For example, allowing http://www.example.com/ lets the user view all pages in www.example.com. However, blocking http://www.example.com/banned/ prevents the user from viewing content stored in www.example.com/banned/, including all subfolders in /banned/ (but allows the user to view pages in www.example.com that are not in /banned/).

9 Click Apply Now.

Allowing Access Only to Specific Websites

You can use Workgroup Manager to allow access only to specific websites on computers with Mac OS X v10.5 or later.

If the user tries to visit a website that he or she is not allowed to access, the web browser loads a webpage that lists all sites the user is allowed to access.

To help direct users to allowed sites, the user's bookmarks are replaced by the websites you allow access to. The bookmarks created by allowing access to websites are called *managed bookmarks*.

If the user syncs bookmarks with MobileMe, the first time the user syncs he or she is asked if MobileMe should merge or replace its bookmarks with the managed bookmarks. If the user merges bookmarks, the MobileMe bookmarks will include the original MobileMe bookmarks and the managed bookmarks. If the user replaces bookmarks, the MobileMe bookmarks will include only the managed bookmarks.

You can also use Workgroup Manager to block specific websites instead of blocking all websites. For more information, see "Preventing Access to Adult Websites" on page 231.

To allow access only to specific websites:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Parental Controls and then click Content Filtering.
5. Set the management setting to Always.
6. Select "Limit access to websites by" and choose "allowing access to the following websites only."
7. Use one of the following methods to add websites that you want to allow access to:
   - In Safari, open the site and then drag the icon from the address bar (of Safari) to the list.
   - In Safari, choose Bookmarks > Show All Bookmarks, then drag icons from the bookmark list to the list in Workgroup Manager.
   - If you have a .webloc file of the website you want to allow access to, drag the file into the list.
   - If you don't have a .webloc file of the website you want to allow access to, click the Add (+) button and enter the URL of the website you want to allow.

     In the "Web site title" field, name the website. In the Address field, enter the highest level URL of the site.

     For example, allowing http://www.example.com/ lets the user view all pages in www.example.com. Allowing http://www.example.com/allowed/ lets the user view content stored in www.example.com/allowed/, including all subfolders in /allowed/, but not folders located outside of /allowed/.
8. To create folders to organize websites, click the New Folder (folder) button, then double-click the folder to rename it.

   To add URLs within a folder, open the folder's disclosure triangle, select the folder, and then click the Add (+) button.

   To create a subfolder, open a folder's disclosure triangle, select the folder, and then click the New Folder (folder) button.
9. To change the name or URL of a website, double-click the website entry; then, to rename a folder, double-click the folder entry.
10. To rearrange websites or folders, drag the websites or folders within the list.
11. Click Apply Now.

Setting Time Limits and Curfews on Computer Usage

You can use Workgroup Manager to set time limits and curfews for computer usage on computers with Mac OS X v10.5 or later.

If you set a time limit for computer usage, users who meet their daily time limits can't log in until the next day when their quota is reset. You can set different time limits for weekdays (Monday through Friday) and weekends (Saturday and Sunday). The time limit can range from 30 minutes to 8 hours.

If you set a curfew, users can't log in during the days and times you specify. If a user is logged in when their curfew starts, the user is immediately logged out. You can set different times for weekdays (denying access Sunday nights through Thursday nights) and weekends (Friday and Saturday nights).

To set time limits and curfews:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Parental Controls and then click Time Limits.
5. Set the management setting to Always and then select "Enforce limits."
6. To set time limits, click Allowances, then under Weekdays or Weekends select "Limit computer use to" and drag the slider to the amount of time you want to limit use.
7. To set curfews, click Curfews, select "Sunday through Thursday" or "Friday and Saturday," and then enter the range of time when you want to prevent computer access.

   You can highlight the time and replace it with a new time, or you can highlight the time and click the up or down buttons next to the time.
8. Click Apply Now.

Managing Printing Preferences

Use Printing preferences to create printer lists and manage access to printers.

The table below describes what the printing settings do.

Printing preference pane	What you can control
Printers	Available printers, the user's ability to add printers or access a printer, and the default printer
Footer	Customization of the page footer

Making Printers Available to Users

You can set up a managed printer list so that users, groups, or computers have a specific set of network printers available when they print.

The list of printers available to the user is a combination of managed printers for the user, the group selected at login, and the computer used, and any printers that are add to the printer list on the user's computer. You can restrict the printer list to only show managed printers.

Printers added using AppleTalk are not supported for client computers running Mac OS X v10.6.

To create a printer list for users:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Printing and then click Printers.
5. Set the management setting to Always.
6. Click Printer List.

   The Available Printers list is created from the list of available network printers in Print & Fax System Preferences.
7. Select a printer in the Available Printers list and then click "Add" 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 the Printer & Fax printer list.
8. To restrict the printer list to only show managed printers, select "Only show managed printers."
9. Click Apply Now.

Preventing Users from Modifying the Printer List

If your users run Mac OS X v10.5, they must authenticate as local administrators to change the list of printers.

If your users run Mac OS X v10.6 or later or Mac OS X v10.4 or earlier, you can manage preferences so users don't need to authenticate as local administrators to change the list of printers.

To restrict access to the printer list:

1. In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Printing and then click Printers.

5 Set the management setting to Always.

6 Click Printer List.

7 Deselect "Allow user to modify the printer list."

8 Click Apply Now.

Restricting Access to Printers Connected to a Computer

In some situations, you might want only specific 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 by making the teacher an administrator and requiring an administrator's user name and password to access the printer.

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

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Printing and then click Printers.

5 Set the management setting to Always.

6 Click Printer List.

7 If you want the client computer to have access to a network printer, select the printer and then click "Add to List."

8 If you don't want users to access local printers, deselect "Allow printers that connect directly to the user's computer."

9 To require an administrator password to use the printer, select "Require an administrator password."

10 Click Apply Now.

Setting a Default Printer

After you set up a printer list, you can specify a printer as the default printer. When a user tries to print a document, this printer is the preferred selection in an application's print dialog.

To set the default printer:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Printing and then click Printers.
5. Set the management setting to Always.
6. Click Access.
7. Select a printer listed in User's Printer List and then click Make Default.
8. Click Apply Now.

Restricting Access to Printers

You can require an administrator user name and password to print to specific printers.

To restrict access to a specific printer:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Printing and then click Printers.
5. Set the management setting to Always.
6. Click Access, select a printer listed in User's Printer List, and then select "Require an administrator password."
7. Click Apply Now.

Adding a Page Footer to All Printouts

Adding page footers to all printouts can help users identify their printouts from other users printouts. This is especially useful in educational environments where students might print identical or nearly identical assignments.

The footer appears at the bottom left of the page. It overlays existing printed content. If your printouts have footers or very small margins, the managed footer might become garbled.

The footer includes the user's long name and the date and time when the user sent the print job. The date and time is based on the user's computer's date and time, not the server's.

The footer can also include the Ethernet ID of the computer that sent the print job.

For example, here's a footer for a user named Anne Johnson:

Anne Johnson Saturday March 3, 2007 5:59:01 PM PT 00:11:22:33:44:55

To add a footer to all printouts:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Printing and then click Footer.
5. Set the management setting to Always.
6. Select "Print page footer (user name and date)."
7. To print the Ethernet ID, select "Include MAC address."
8. Choose a font for the footer from the Font name pop-up menu.

   You can choose Helvetica, Courier, Lucida Grande, or Times.
9. Enter a font size for the footer.

   There is no font size limit for the footer. However, 7 is the default (and recommended) size.
10. Click Apply Now.

Managing Software Update Preferences

With Mac OS X Server, you can create a Software Update server to control updates that are applied to specific users or groups. This is helpful because it reduces external network traffic while also providing more control to server administrators.

By configuring the Software Update server, server administrators can choose which updates to provide.

To manage access to Software Update servers:

1. In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Software Update.

5 Set the management setting to Always.

6 Specify a URL in the form http://someserver.apple.com:8088/index.sucatalog.

7 Click Apply Now.

Managing Access to System Preferences

You can specify which preferences to show in System Preferences.

If a user can see a preference, it does not mean the user can modify that preference. Some preferences, such as Startup Disk preferences, require an administrator name and password before a user can modify its settings.

The preferences that appear in Workgroup Manager are those installed on the computer you're currently using. If your administrator computer is missing preferences that you want to disable on client computers, install the applications related to those preferences or use Workgroup Manager on a computer that includes those preferences.

To manage access to System Preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click System Preferences.

5 Set the management setting to Always.

6 For each item you don't want to appear in a user's System Preferences, deselect its Show checkbox.

To select all Show checkboxes, click Show All. To deselect all Show checkboxes, click Show None.

7 Click Apply Now.

Managing Time Machine Preferences

Time Machine preferences let you control Time Machine, which provides a backup of computer data to network servers. Time Machine backs up all computer data, such as installed applications and their preferences, all local account data, and (optionally) system files. To use Time Machine, your computers must run Mac OS X v10.5 or later.

To manage Time Machine, you must run file services, such as AFP service. When managed users log in to Mac OS X, their login name and password are used to authenticate them with the file server.

You can back up a computer's startup volume or all local volumes. If users have network accounts, their data isn't backed up through Time Machine (because their data is stored on a network server, not locally).

You can enable Time Machine to perform automatic hourly backups. If you don't use automatic backup, the user can manually back up using Time Machine.

Time Machine is useful for backing up computers with primarily local accounts. It is also useful if users have administrative control over the computer and can install their own applications.

You can limit the total backup storage per computer. When you limit total backup storage for a computer group, the limit applies to each computer in it. If you limit a computer group to 2 GB, and the computer group has five members, the computer group can use up to 10 GB of backup storage. Backup storage is not preallocated, so the server can run out of space before the computers reach their backup storage limit.

If a user runs out of backup storage, Time Machine stops backing up data. To make sure Time Machine doesn't run out of space, make the limit larger than the expected size of the data being backed up, and don't back up system files.

You can save space on the file server by not backing up system files. System files include files that are created when Mac OS X is installed. If you don't back up system files and system files are corrupted, you must use the Mac OS X Server installation discs to reinstall Mac OS X Server. By not backing up system files, you speed up the initial backup but you don't speed up subsequent backups.

To manage Time Machine preferences:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more computers or computer groups.
4. Click Time Machine.

5 Set the management setting to Always.

6 In the "Backup server" field, enter the URL of the file server or share point that will store Time Machine backups, using the form afp://www.example.com/Backups/.

Replace www.example.com/Backups/ with the URL of the file server or share point. The location you enter must already exist.

7 To select volumes to back up, select "Startup volume only" or "All local volumes."

8 To back up system files, deselect "Skip system files."

9 To use automatic backup, select "Back up automatically."

10 To limit backup storage, select "Limit total backup storage to: # MB" and replace # with the number of MB to limit backup storage.

11 Click Apply Now.

Managing Universal Access Preferences

Universal Access settings can help improve the user experience. For example, if a user 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 can set up and manage Universal Access settings for specific workgroups or computers dedicated to users with special needs.

The table below describes what the settings in each Universal Access pane can do.

Universal Access preference pane	What you can control
Seeing	Visual display and desktop zooming
Hearing	Visual alert for users
Keyboard	How the keyboard responds to keystrokes and key combinations
Mouse	How the pointer responds, and whether users can use the numeric keypad instead of a mouse
Options	Shortcut key combinations, the use of assistive devices, and whether the computer reads text in the Universal Access preference pane

Adjusting the User's Display Settings

The Seeing settings in Universal Access preferences alter the appearance of the screen. The user can easily zoom in or out on the desktop using keyboard shortcuts (specific key combinations). Changing to grayscale or white-on-black display can sometimes make it easier to read text on the screen.

Note: If display settings are managed Once, users can switch between the zoom or color options using keyboard shortcuts. If the management setting is Always, users can't switch between options.

To further customize the user's display, you can use Finder Views 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. For more information, see "Managing Finder Preferences" on page 193 and "Managing Dock Preferences" on page 185.

If you plan to manage dedicated computers, you might be able to use local Display System Preferences to change the resolution and number of colors computers use. After setting the resolution and number of colors, you can prevent changes to the Display System Preferences by removing Display from the list of available System Preferences.

For more information, see "Managing Access to System Preferences" on page 239.

For more information about enabling assistive devices like screen readers, see "Allowing Devices for Users with Special Needs" on page 245.

To adjust screen appearance:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Universal Access.
5. Click Seeing and then select a management setting.
6. To enable zooming, select "Turn on Zoom"; to fine-tune zoom settings, click Zoom Options.

   Use the sliders to set a maximum 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."
7. To change the color scheme to white on black or grayscale, select "Switch to" and then select "White on Black" or Grayscale.
8. Click Apply Now.

Setting a Visual Alert

If users can't hear computer alert sounds (for example, the sound played when new mail arrives or an error occurs), you can flash the screen as an alternative.

To set a flashing alert:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Universal Access.
5. Click Hearing and then select a management setting.
6. Select "Flash the screen whenever an alert sound occurs."
7. Click Apply Now.

Adjusting Keyboard Accessibility Options

If some users have difficulty pressing keys, you can use Sticky Keys or Slow Keys to help them use the keyboard.

Sticky Keys help users who can't press multiple keys simultaneously. It treats a sequence of modifier keys (Shift, Command, Option, and Control) like a key combination. For example, to press Command-O, users can press Command and then O.

To hold down a key with multiple keystrokes, users can press the key twice. For example, pressing Shift twice is like using Caps Lock, except that it also presses Shift when entering commands. So if you've pressed Shift twice, and you press Command and then O, it's the same as pressing Shift-Command-O (because using Caps Lock instead of pressing Shift twice is like pressing Command-O). Pressing Shift a third time removes the Shift key from the current key combination.

If you set up Sticky Keys, you can make them more useful by enabling these options:

Option	Effect
Beep when a modifier key is set	Setting and holding a modifier key makes distinct typewriter sounds. Removing a key from the current key combination doesn't create a sound.
Display pressed keys onscreen	When a modifier key is pressed, a silhouette of the modifier key is shown onscreen. If the modifier key is only active for a single press, its silhouette is dim. If the modifier key is in held-down mode, its silhouette is bright.

Slow Keys help users who press keys for too long or accidentally press keys. If you enable Slow Keys, you can set a delay when a key is accepted. If the user presses a key for less time than the acceptance delay, the keystroke isn't accepted.

To help users recognize when their keystrokes are accepted, enable the "Use click sounds" option to play a sound when the user initially presses a key and a different sound when the key is accepted.

Note: If you enable Universal Access Shortcuts, a user can press the Shift key five times to turn Sticky Keys on or off. For more information, see "Enabling Universal Access Shortcuts" on page 245.

To set the way the keyboard responds to keystrokes:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click Universal Access.
5. Click Keyboard and then select a management setting.
6. To activate Sticky Keys, select Sticky Keys On.

   To turn off the key-combination alert, deselect "Beep when a modifier key is set."

   To turn off onscreen display of keystrokes, deselect "Show pressed keys on screen."
7. To activate Slow Keys, select Slow Keys On.

   If you don't want audio feedback during keystrokes, deselect "Use click key sounds."

   Move the slider to adjust the amount of delay between when a key is pressed and when the computer accepts it.
8. Click Apply Now.

Adjusting Mouse and Pointer Responsiveness

If some users can't use a mouse (or prefer not to), the Mouse Keys feature allows them to use the numeric keypad instead. Keys on the numeric keypad correspond to directions and mouse actions so the user can move the pointer and hold, release, or click.

Note: If you enable Universal Access Shortcuts, a user can press the Option key five times to turn Mouse Keys on or off.

If the pointer moves too quickly for some users, you can adjust how soon the pointer begins to move and how fast it moves.

To control mouse and pointer settings:

1. In Workgroup Manager, click Preferences.
2. Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Universal Access.

5 Click Mouse and then select a management setting.

6 To activate Mouse Keys, select Mouse Keys On.

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 onscreen zooming or enabling Sticky Keys.

If you choose not to allow Universal Access shortcuts, users might not be able to use features such as Zoom or turn off activated features such as Sticky Keys.

To allow Universal Access Shortcuts:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

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

4 Click Universal Access.

5 Click Options and then set the management setting to Once or Always.

6 Select Allow Universal Access Shortcuts.

7 Click Apply Now.

Allowing Devices for Users with Special Needs

You can allow managed users to turn on assistive devices, such as a text reader.

To allow assistive devices:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3 Select one or more computers or computer groups.

4 Click Universal Access.

5 Click Options and set the management setting to Always.

6 Select "Enable access for assistive devices."

7 Click Apply Now.

Using the Preference Editor with Preference Manifests

Workgroup Manager includes a preference editor, which you can use to control any Mac OS X application or utility developed using Apple standard conventions for handling preferences.

You can also use it to manage preferences that are not configurable in the Workgroup Manager main preferences interface.

As with the main preferences interface, you can use the preference editor to manage preferences for users, groups, computers, and computer groups.

For example, in Safari you can disable JavaScript by setting the JavaScript Enabled key to "false." If you save this key in the Often group, the user can enable JavaScript during their current login session but JavaScript is disabled when the user logs out and logs in again.

Some application developers provide *preference manifests*. A preference manifest simplifies modification of preferences by providing names and descriptions of keys that are honored by an application, and tells you how to set them.

Preference manifests are similar to templates. They're not required, so you can edit the preference key value of an application even if it doesn't provide a preference manifest. For applications without preference manifests, you can import a preference file from ~/Library/Preferences, or you can import the application (and its preference file is found automatically).

Preference manifests can be stored in an application package (a file ending with .manifest, such as com.apple.Safari.manifest, in the package's /Contents/Resources/ folder), or they can be standalone files. If manifests exist for an application, the preference editor loads them when you add the application to the preference editor's list.

When you import preferences for an application, keys and values are added based on the application's currently set preferences. This lets you apply your own configuration of applications to users' applications.

You can add, remove, or edit keys, but some keys might not be well described if the application doesn't have a preference manifest or if the key you're editing isn't in the preference manifest.

Adding to the Preference Editor's List

Before you can manage an application in the preference editor, you must add the application or the application's preference file to the preference editor's list. The application's preference file is in ~/Library/Preferences/.

You can manage any application that uses Mac OS X preferences. To do this you must set preferences for a local copy of that application stored on the administration computer. Then you can add the .plist file for the application stored in ~/Library/Preferences/ to the preference editor's list.

You can also import application preferences when you add the application to the preference editor's list.

When you use your own application preferences, you can choose the management frequency applied to those preferences:

Frequency	Description
Once	Similar to the Once setting in the main interface. Sets a preference but allows the user to change that preference and retain his or her changes.
Often	Only available in the preference editor. Allows users to modify their preferences but the preferences revert to your managed setting every time the user begins a new session.
Always	Similar to the Always setting in the main interface. Sets a preference and usually does not allow the user to modify the preference.

Some applications use ByHost preferences. These preferences apply to a specific user for a specific computer. For example, if a network user sets screen saver preferences, they are saved as ByHost preferences. The user's screen saver preferences are saved for the current computer but are not applied when the user uses other computers.

If users typically run Mac OS X v10.5 or later, it's usually a good idea to import preferences as ByHost preferences. If users typically run earlier versions of Mac OS X, don't import preferences as ByHost preferences.

Some applications use but don't properly respect ByHost preferences. Test your settings with "Import as ByHost preferences" selected and deselected to see if the application you're managing respects ByHost preferences.

To add to the preference editor's list:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.

3. Select one or more users, groups, computers, or computer groups.
4. Click the Add (+) button.
5. Select an application in /Applications, or a .plist file located in ~/Library/Preferences/.

   Applications without preference manifests appear in italics.
6. If you've selected an application and set preferences for it, you can select "Import my preferences for this application."
7. Choose a management setting from the "Manage imported preferences" pop-up menu.

   If you've selected a preference file located in ~/Library/Preferences/ByHost and you've chosen Once or Often from the "Manage imported preferences" pop-up menu, you can select "Import as ByHost preferences."
8. Click Add.
9. If you're asked to replace the manifest, click Replace to replace the manifest.

   Replacing the manifest changes the underlying manifest file for the application but it doesn't change existing managed preferences.
10. If you're asked to replace the managed preferences, click Replace to remove existing managed preferences and replace them with preferences from the application you're adding.

Editing Application Preferences with the Preference Editor

You can use the Workgroup Manager preference editor to edit and manage application-specific preferences.

An application that follows Apple standard conventions for handling preferences will respect the settings in a preference manifest. For applications without preference manifests, test your settings to make sure they produce the desired results.

Before using the preference editor to manage application preferences, add the application or its preference file to the preference editor's list. For instructions, see "Adding to the Preference Editor's List" on page 247.

The preference editor divides keys by management frequency, as described below.

Frequency	Description
Once	Similar to the Once setting in the main interface. Sets a preference but allows the user to change that preference and retain his or her changes.
Often	Only available in the preference editor. Allows users to modify their preferences but the preferences revert to your managed setting when a user begins a new session.
Always	Similar to the Always setting in the main interface. Sets a preference and usually does not allow the user to modify the preference.

Note: Always might still allow users to modify preferences. For this reason, Often is usually a better choice for making persistent preference changes.

Important: When you add or modify keys, always test the additions or changes to make sure they work as expected.

To edit application preferences:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Select an item in the list and click the Edit (pencil) button.
5. To locate the keys you want to change, click the disclosure triangles.
6. To add a key to the application's preferences file, click the disclosure triangle for the frequency, select the frequency, click New Key, click the New Item entry that is created, and choose a key from the pop-up menu, or choose Edit and enter a new key.

   If you don't click the disclosure triangle and select the frequency, the New Key button is deactivated.
7. To change the key's current settings, click the key's type or value.

   If you change the type to a setting that is not by default enabled by the preference manifest, the preference file editing screen indicates the mismatch with an arrow icon. This does not prevent you from changing the key type or value.
8. Click Apply Now and then click Done.

Removing an Application's Managed Preferences in the Preference Editor

You can remove all managed preferences for any entry in the preference editor's list.

If you added an application without a preference manifest, the application is also removed from the preference editor's list when you remove all of its managed preferences.

This action does not delete an application's preference manifest or the application's preferences file. To remove all preference manifests from Workgroup Manager, close Workgroup Manager and delete ~/Library/Preferences/com.apple.mcx.manifests.

To disable management of an application's preferences:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Select an entry with managed preferences.

   Entries with managed preferences are noted by a cursor icon in the left column.

   This can only be done one entry at a time.
5. Click the Remove (–) button and then click Remove in the confirmation dialog.

Using the Preference Editor to Manage Core Services

You can add several important manifests by adding a single core services bundle. These manifests allow management of many features that are unavailable through the main preference editing interface.

For example, you can disable Bluetooth, lock iTunes parental controls, and set the license number and registration key for all iWork '08 installations.

Core service manifests include:

Manifest	Examples of things you can change
Bluetooth	Enable or disable Bluetooth.
Dashboard	Enable or disable Dashboard.
Desktop Picture	Set the Desktop background image.
Dock	Customize how the Dock looks.
Folder Redirection	Save cached files to /tmp on the local computer. This can reduce network traffic. You can't redirect folders to a network location.
Home Sync	Fine-tune mobility settings, such as how to resolve conflicts.

Manifest	Examples of things you can change
iCal	Change iCal settings such as Kerberos usage, SSL usage, and refresh intervals.
iChat	Change iChat settings such as account name and info, and SSL and Kerberos usage.
Internet Configuration	Change Internet settings such as the mail server, mail information, default web browser, and default mail application.
iTunes	Set iTunes parental controls and enable or disable podcasts and music sharing.
iWork Registration	Set iWork '08 registration information.
Kerberos Login	Set Kerberos name and realm.
Menu Extras	Add nonstandard menus to the menu bar.
Mobile Account & Other Options	Change mobile account settings like FileVault use, enable sync encryption, set mobile account lifetime, and customize the mobile account creation dialog.
Quicktime Pro Key	Set QuickTime registration information.
Screen Saver	Set screen saver settings.
Sidebar	Add custom locations such as /Users/Shared/ to the sidebar in Finder.
Sleep & Screen Saver Password	Enable or disable screen saver passwords.
VPN Settings	Change VPN settings such as VPN server information, login name, and authentication type.

By default, these manifests don't show keys. You must click the disclosure triangle next to the frequency, select the frequency, and then click New Key. When you click the name of the new key, you'll see all available keys for that frequency.

Some keys only work with specific management frequencies. For example, you can only enable "Disable Bluetooth" by adding a new key with the frequency Always.

To add the core services bundle to the preference editor list:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click the Add (+) button.
5. Select /System/Library/CoreServices/ManagedClient.app and click Add.

Using the Preference Editor to Manage Safari

Safari is a good example of an application that can be managed by editing its preference manifest.

The Safari version included with Mac OS X v10.5 or later is more configurable than previous versions of Safari. It includes more than 30 configurable preferences, including:

- Home Page
- Default Font
- Command-Click Makes Tabs
- AutoFill Passwords
- AutoFill Credit Cards
- Java Enabled
- JavaScript Enabled
- Ask Before Submitting Insecure Forms

When you add Safari to the preference editor list, two entries are added. The com.apple.Safari preference manifest includes most configurable preferences, while com.apple.WebFoundation includes a configurable preference for the cookie acceptance policy.

By default, these manifests don't show any keys. You must click the disclosure triangle next to the frequency, then select the frequency and click New Key. When you click the name of the new key, you see available keys for that frequency.

To add Safari to the preference editor list:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click the Add (+) button, select /Applications/Safari, and then click Add.

   The preference manifests included with older versions of Safari don't have as many configurable preferences as the Safari version included with Mac OS X v10.5 or later. You can replace old Safari preference manifests by adding the new Safari application, and then clicking Replace in the dialog that appears.
5. To edit Safari preferences, select Safari (with the Preference ID com.apple.Safari), click the Edit (pencil) button, and then add keys you'd like to manage.

   For more information, see "Editing Application Preferences with the Preference Editor" on page 248.

Using the Preference Editor to Manage Apple Remote Desktop

You can manage Apple Remote Desktop (also known as *Remote Desktop*) report settings for computers or computer groups in the preference editor. You must have Remote Desktop v3.3 or later installed on your administrator computer.

When you add Remote Desktop to the preference editor list, three preference manifests are added:

Manifest	Examples of things you can change
com.apple.ARDAgent	Task server white list and reporting cache policy.
com.apple.RemoteDesktop	Advanced Remote Desktop application settings, encryption settings, report scheduling settings and enabled report types.
com.apple.RemoteManagement	Network settings, computer control, and display settings.

By default, these manifests don't show any keys. You must click the disclosure triangle next to the frequency, then select the frequency and click New Key. When you click the name of the new key, you see available keys for that frequency.

To add Apple Remote Desktop to the preference editor list:

1. In Workgroup Manager, click Preferences and then click Details.
2. Make sure the correct directory is selected and you are authenticated.

   To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory administrator.
3. Select one or more users, groups, computers, or computer groups.
4. Click the Add (+) button, select /Applications/Remote Desktop, and then click Add.
5. To edit Remote Desktop preferences, select a Remote Desktop entry in the list, click the Edit (pencil) button, and then add keys you'd like to manage.

   For more information, see "Editing Application Preferences with the Preference Editor" on page 248.

Managing Preferences from the Command Line

To control managed preferences, use managed client (MCX) extensions with the `dscl` command. You can use the `mcxquery` command to view effective managed preferences for users, workgroups, and computer groups. You can use the `mcxrefresh` command to make managed preferences take effect immediately, even while a user is logged in.

Using MCX Extensions

Although you can use other `dscl` commands to control managed preferences, using MCX command extensions with `dscl` provides an easier way. You can use these extensions in interactive or command-line modes.

The `dscl` command provides the following MCX extensions:

Extension	Description
`-mcxread`	Displays the existing values of an MCX preference key.
`-mcxset`	Sets the value of an MCX preference key.
`-mcxedit`	Updates the value of an MCX preference key.
`-mcxdelete`	Removes management for the specified MCX preference keys.
`-mcxexport`	Same functionality as the `-mcxread` command, but stores the output in the specified file using the specified format. The resulting file can later be imported using the `-mcximport` command.
`-mcximport`	Imports the keys and values previously exported using the `-mcxexport` command.
`-mcxhelp`	Displays help information for MCX extensions.

Syntax

These command extensions have the following syntax:

```
-mcxread recordPath [-v mcxVersion] [-o filePath] [-format {xml | plist |
     text}] [appDomain [keyName]]
-mcxset recordPath [-v mcxVersion] appDomain keyName [mcxDomain [keyValue
     [UPK]]]
-mcxedit recordPath [-v mcxVersion] appDomain keyPath [keyValue]
-mcxdelete recordPath [-v mcxVersion] [appDomain [keyName]]
-mcxexport recordPath [-o filePath] [-format {xml | plist | text}]
     [appDomain [keyName]]
-mcximport recordPath [-d] filePath
-mcxhelp
```

Parameter	Description
recordPath	The record in the service directory node to be accessed (for example, `/LDAPv3/127.0.0.1/Users/sam`). This parameter is always required, but if you are in interactive mode, you can use a period to represent the current directory.
mcxVersion	The version of the key to be retrieved. If you omit this parameter, the command searches for version 1 keys.
-format	The format of the output file (XML, plist, or text).
optArgs	(Optional) One or more options.
appDomain	(Optional) An application's domain. For example, the application domain for the Dock is `com.apple.dock`.
keyName	(Optional) The name of the managed preference (for example, `familyControlsEnabled`, `mcx_emailAddress`, and `mcx_defaultWebBrowser`).

Parameter	Description
mcxDomain	(Optional) The type of management applied to the key. Legal values are: • `none` (not managed) • `always` • `once` • `often` • `unset`
keyValue	(Optional) The new value to be used for a key. You can specify this parameter using the same syntax as that of the `defaults` command. For more information, see the man page of the `defaults` command. When specifying plist or xml values, enclose the parameter in single quotes (for example, `'(authenticate, eject)'` and `'<real>64.0</real>'`).
UPK	(Optional) The value for the Union Policy Key (UPK). If present, the UPK *must* be specified as a dictionary. The valid keys for the dictionary include: • `mcx_input_key_names` or `input` (single string or array of strings) • `mcx_output_key_names` or `output`(single string) • `mcx_remove_duplicates` (boolean) • `mcx_union_as_dictionary` (boolean) • `mcx_replace` (boolean) If `mcx_input_key_names` or `mcx_output_key_name` is omitted, the value of *keyName* is used instead.
keyPath	(Optional) The path to a sub-plist in an existing key value. For example, `'mount-controls:dvd:1'` means the second element the array with the key `'dvd'` the key `'mount-controls.'`
filePath	(Optional) The location of the output or input file.
`-d`	The keys found in the import file from the record that should be deleted. This is equivalent to calling `-mcxdelete` for every key in the import file. The value of the key in the import file is ignored.

Example

The following command sets the `autohide` key in the `com.apple.dock` domain to a value of `TRUE` with `always` for management.

```
$ dscl -mcxset /LDAPv3/127.0.0.1/Users/sam com.apple.dock autohide always
     -bool 1
```

The following command removes preference management for the `autohide` key in the `com.apple.dock` domain for the current record:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcxset . com.apple.dock autohide none
```

The following command displays, in plist format, all keys for all application domains for the current record:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcxread . -format plist = =
```

The following command changes the autohide key to `TRUE`, preserving the current management setting:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcxedit . com.apple.dock autohide -boot 1
```

The following command causes the `autohide` Dock key to no longer be managed:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcxdelete . com.apple.dock autohide
```

The following command exports the keys in the `com.apple.dock` domain for the current record to the /tmp/export.plist file:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcxexport . -o /tmp/export.plist com.apple.
     dock
```

The following command imports the keys in the /tmp/export.plist file into the current directory:

```
$ dscl
> cd /LDAPv3/127.0.0.1/Users/sam
/LDAPv3/127.0.0.1/Users/sam > mcximport . /tmp/export.plist
```

For more examples, use the `mcxhelp` extension.

Determining Effective Managed Preferences

You can use Workgroup Manager to configure managed preferences at the user, workgroup, and computer level. Determining the effective managed preferences for a user's computer experience is not easy, especially if the managed user is a member of many managed workgroups and each workgroup is a member of a different computer group.

To simplify the process of determining effective managed preferences, Mac OS X Server provides the `mcxquery` command. You can use this command to determine the effective managed preferences for user, workgroup, or computer group records.

Syntax

```
$ mcxquery options -user userName -group groupName -computer computerName
```

Parameter	Description
options	(Optional) Two options for specifying the name and format of the file where the results of the query (the effective managed preferences) are stored: • `_o fileName`: The name of the output file (including the path) where the results of running this command are stored. • `_format {space | tab | xml}`: The format of the output, which can be space-delimited, tab-delimited, or XML.
userName	(Optional) The short name of a user. If you do not provide the short name for this option or if you use the equal sign (=), this command uses the short name of the logged in console user.
groupName	(Optional) The short name of a workgroup. A value of = indicates the workgroup (if any) chosen for the current login session.
computerName	(Optional) The short name of the computer group, the MAC address of a computer, or the UUID of the computer. If you do not provide a value for this option or if you use the equal sign (=), this command uses the MAC address of the current computer.

Examples

The following example displays the managed preferences for Sam and stores the results in XML format in the samPrefs.out file:

```
$ mcxquery -o samPrefs.out -user sam
```

The following example displays the managed preferences for Jane, who is logged in using the science workgroup from a computer that is a member of the lab1_12 computer group:

```
$ mcxquery -user jane -group science -computer lab1_12
```

The following example displays the managed preferences for Jane, who is logged in using the science workgroup from the computer whose Ethernet MAC address is 11:22:33:44:55:66:

```
$ mcxquery -user jane -group science -computer 11:22:33:44:55:66
```

Manually Refreshing Managed Preferences

You can manually refresh managed preferences for a user. If a user is logged out, the user's preferences are refreshed when the user logs in. If the user is logged in, you must manually refresh managed preferences for the latest changes to apply.

Syntax

```
$ mcxrefresh [-u 'uid'] [-n 'userName']
```

Parameter	Description
uid	(Optional) The user ID of the user to be refreshed. If you do not provide the user ID for this option, this command uses the logged in console user.
userName	(Optional) The short name of a user. If you do not provide the short name for this option, this command uses the logged in console user.

Examples

The following examples refresh the managed preferences for a user with the short name ajohnson, and user ID 1007:

```
$ mcxquery -uid 1007
$ mcxquery -n 'ajohnson'
```

Solving Problems

11

If you encounter problems as you work with Workgroup Manager, you may find a solution in this chapter.

If the answer to your question isn't here, try searching Workgroup Manager Help for new topics. You can also search the Apple Service & Support website for information and solutions at www.apple.com/support/.

Diagnosing Common Network Issues

Before you try the solutions in this chapter, make sure your network is properly configured.

In particular, test your Network Time Protocol (NTP), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) services.

For more information about NTP, DNS, or DHCP, see *Network Services Administration*.

Testing Your Network's Time and Time Zones

The many technologies and services in Mac OS X Server rely on having accurate time settings on all networked computers.

Typically, computers are connected to an NTP server that provides accurate time settings. You should still check your networked computers' time settings using Apple Remote Desktop (not included with Mac OS X Server). For more information about Apple Remote Desktop, see www.apple.com/remotedesktop.

You can send the commands in the following procedure using the `ssh` command. You can also test and correct a computer's time settings in System Preferences. Both methods allow you to test and correct one computer at a time, but with Apple Remote Desktop you can test and correct many computers simultaneously.

To test your network computer time and time zones using Apple Remote Desktop:

1. In Apple Remote Desktop, send the following UNIX command to all computers:

```
sudo systemsetup -gettimezone
```

Your computers should be set for the same time zone. If not, send the following UNIX command:

```
sudo systemsetup -settimezone 'US/Pacific'
```

Replace *US/Pacific* with your time zone. For other time zones, see the man page for `systemsetup`. For instructions on sending UNIX commands through Apple Remote Desktop, see the *Apple Remote Desktop Administrator's Guide*.

2 In Apple Remote Desktop, send the following UNIX command to all computers:

```
sudo systemsetup -gettime
```

Your computers should have times within a few minutes of each other. If they have a range of times, send the following UNIX command:

```
sudo systemsetup -settime current_time
```

Replace *current_time* with the current time in 24-hour format, using *HH:MM:SS* (hour, minute, second) notation.

Testing Your DNS Service

Your DNS service should allow you to discover a server's domain name when given an IP address, or to retrieve an IP address when given a domain name. If your computers can't do these tasks, perform further analysis on your DNS service. For a detailed description of DNS and for instructions on configuring DNS, see *Network Services Administration*.

If you have Apple Remote Desktop installed, you can quickly test your entire network. In Apple Remote Desktop, create a scanner that displays computers with IP addresses in the range distributed by your DHCP server. If a computer is turned on, is not in sleep mode, and is connected to your network, the computer should appear in the scanner.

The scanner displays the IP address given to the computer and the computer's host name. Computers that are not assigned host names by the DNS service are listed without host names. If a computer is listed and has a valid IP address and host name, the computer is receiving DHCP and DNS service.

For more information about how to use scanners in Apple Remote Desktop, see the *Apple Remote Desktop Administrator's Guide*.

If you do not have Apple Remote Desktop installed, you can perform the following task to test a single computer's ability to receive DNS service.

To test DNS on a single computer:

1 On a network computer that is not the server providing DNS service, open Network Utility.

2 In the Lookup pane of Network Utility, enter the domain name of your Open Directory master server and click Lookup.

The resulting log should have an answer section, which displays the IP address of your Open Directory master server. If there is no answer section, or if the IP address is incorrect, perform further analysis on your DNS service.

3 In the Lookup pane of Network Utility, enter the IP address of your Open Directory master server and click Lookup.

The resulting log should display the domain name of your Open Directory master server. If the domain name is incorrect, perform further analysis on your DNS service.

Note: Instead of using Network Utility, you can use the `dig` tool in Terminal. Enter the following command in Terminal:

```
dig name_or_address
```

Replace *`name_or_address`* with the domain name or the IP address of your Open Directory master server. The resulting log should have an answer section with the correct IP address or domain name.

Testing Your DHCP Service

Your DHCP service should be configured to supply enough IP addresses to serve your network. If a computer does not have a valid IP address, it can't be contacted through your network. For a detailed description of DHCP and for instructions on configuring DHCP, see *Network Services Administration*.

If you have Apple Remote Desktop installed, you can quickly test your entire network. In Apple Remote Desktop, create a scanner that displays computers with IP addresses in the range distributed by your DHCP server. If a computer is turned on, is not in sleep mode, and is connected to your network, the computer should appear in the scanner.

The scanner displays the IP address given to the computer and the computer's host name. Computers that are not assigned host names by DNS are listed without host names. If a computer is listed and has a valid IP address and host name, the computer is receiving DHCP and DNS service.

For more information about how to use scanners in Apple Remote Desktop, see the *Apple Remote Desktop Administrator's Guide*.

If you do not have Apple Remote Desktop installed, you can perform the following task to test a single computer's ability to receive DHCP service.

To test DHCP on a single computer:

1 In Server Admin, click the disclosure triangle at the left of the server providing DHCP service.

This displays all of the server's services.

2 Select DHCP and click Subnets.

The Subnets pane lists the addresses your DHCP server supplies.

3 On a client computer, open Network Utility, click Info, and then select the network interface that connects to your network.

If the displayed IP address is not in your range of supplied addresses, the computer is not receiving an IP address through your DHCP service.

If the IP address is 169.254.x.x, it is a self-assigned IP address. This means your computer is not receiving DHCP service.

If the IP address is not an assigned address and is not 169.254.x.x, the computer is receiving DHCP service from a DHCP server other than yours.

Solving Account Problems

Follow the suggestions in this section when problems arise with user and group account administration.

If You Want to Use Earlier Versions of Workgroup Manager

If you have administrative applications and tools from Mac OS X Server v10.4 or earlier, do not use them with Mac OS X Server v10.5 or later.

You can use Mac OS X Server v10.6 applications to administer Mac OS X Server v10.4.11 or later.

If You Can't Edit an Account Using Workgroup Manager

Editable domains include the local directory domain, Open Directory domains, and other read/write directory domains.

Before you can edit an account using Workgroup Manager, authenticate as a directory administrator. To authenticate, click the lock near the top of the Workgroup Manager window.

If Users Can't See Their Names in the Login Window

When you upgrade Mac OS X and migrate users to a shared directory on the new server, some users might not appear in the login window. The login window does not list system users, but they can still log in by entering their user names and passwords.

The login window lists users depending on how Login preferences are managed. For more information, see "Changing the Appearance of the Login Window" on page 201.

If You Can't Unlock an LDAP Directory

To make changes in a directory domain, you must authenticate with the name and password of a directory administrator. Therefore, to edit an entry in a shared LDAPv3 directory domain, you must authenticate in Workgroup Manager using the name and password of an administrator account in that LDAPv3 directory domain.

You can't use an administrator account in the computer's local directory domain to authenticate as an administrator of a shared LDAP directory.

If 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 where the user's record resides. In addition, your user account must have a password type of Open Directory.

Setting up an Open Directory master (using Server Assistant or the Open Directory service settings in Server Admin) creates a directory administrator account with an Open Directory password. You can use this account to set up other user accounts as directory administrators with Open Directory passwords.

If 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 where the user's record resides. In addition, your user account must be configured for Open Directory authentication.

When the Open Directory master is set up (using the Open Directory service settings in Server Admin) the initial user account is a directory administrator account with an Open Directory password. You can use this account to set up other user accounts as directory administrators with Open Directory passwords.

If You Can't Assign Server Administrator Privileges

To assign server administrator privileges to a user on a server, connect to the server in Workgroup Manager and authenticate in the directory domain. Select the user's account (or create an account for the user), and then select "User can administer this server" in the Basic pane.

If Users Can't Log In or Authenticate

If a user can't log in or authenticate to his or her account, consider the following to determine whether the source of the authentication problem is configuration-related or due to the password:

- Reset the password to a known value and then determine whether there is still a problem. Try using a 7-bit ASCII password, which is supported by most clients.
- Make sure the password contains characters supported by the authentication protocol. Leading, embedded, and trailing spaces, as well as special characters (such as pressing Option-8 to form a bullet), are not supported by some protocols. For example, leading spaces work with POP and AFP, but not IMAP.
- Make sure the user's keyboard can generate all characters in the user's password.
- Crypt passwords don't support many authentication methods. To increase the probability that a user's client applications are supported, set the user's password type to Open Directory or suggest that the user try a different application.

- If the user's account resides in a directory domain that is not available, create a user account in a directory domain that is available.
- Make sure the client software encodes the password so it is recognized correctly. For example, Open Directory recognizes UTF-8 encoded strings, which might not be sent by some clients.
- Make sure 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 causes an authentication failure even though Windows service supports longer passwords.
- If you disabled authentication methods for Open Directory or shadow passwords (such as APOP or LAN Manager) the user's applications can't authenticate using the disabled methods.

  After enabling or disabling Open Directory Password Server or shadow password authentication methods, you might need to reset the user's password.

  For information about enabling and disabling authentication methods, see *Open Directory Administration*.
- For Kerberos troubleshooting tips, see "If Users Can't Authenticate Using Single Sign-On or Kerberos" on page 266.
- If a Mac OS v8.1–8.6 computer fails to authenticate for Apple file service, the computer's AppleShare Client software might need upgrading:
  - Mac OS v8.6 computers should use AppleShare Client v3.8.8.
  - Mac OS v8.1–8.5 computers should use AppleShare Client v3.8.6.
  - Mac OS v8.1–8.6 computers that have file server volumes mount during startup should use AppleShare Client v3.8.3 with DHX UAM (User Authentication Module) installed. DHX UAM is included with the AppleShare Client v3.8.3 installation software.

If Users Relying on a Password Server Can't Log In

If your network has a server with Mac OS X Server v10.2, it could receive authentication from an Open Directory password server hosted by another server. If the password server's computer disconnects 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 their server's 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. Alternately, while the password server's computer is offline, users can log in with user accounts whose password type is crypt or shadow password.

If 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 can become inaccessible due to a problem with the network, the server software, or the server hardware.

Problems with the server hardware or software affect users trying to log in to Mac OS X computers and users trying to log in to the Windows domain of a Mac OS X Server primary domain controller (PDC). Network problems might 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. Users affected by these problems can log in using a local user account defined on the computer, such as the user account created during setup after installing Mac OS X.

If Users Can't Access Their Home Folders

Make sure users can access the share point where their home folders are located, and make sure they can access their home folders. Users need Read access to the share point and Read & Write access to home folders.

If Users Can't Change Their Passwords

Users who have accounts in the server's LDAP directory with a crypt password can't change passwords after logging in.

These users can change passwords if you use the 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 must instruct users to log in using this new password and have them change it in the Accounts pane of System Preferences.

If Users Can't Authenticate Using Single Sign-On or Kerberos

There are several ways to remedy Kerberos authentication failures. You can find these solutions, as well as a full description of how to reconfigure a server's computer record for single sign-on and Kerberos authentication, in *Open Directory Administration*.

If You Can't Set User Wiki and Blog Settings

In Mac OS X Server v10.6 and later, users can create and manage their own wikis and blogs live on the wiki server. These wikis and blogs are no longer tied to Open Directory groups. Users can freely create wikis and assign access to people who aren't in Open Directory groups. Because users can create and manage their own wikis and blogs live, you can't create wikis and blogs for users in Workgroup Manager.

You can choose which users and groups are allowed to create wikis and blogs in Server Admin. For more information, see *Wiki Services Administration*.

Solving Problems with a Primary or Backup Domain Controller

Problems with a primary domain controller (PDC) or backup domain controller (BDC) can have several causes.

If a Windows User Can't Log in to the Windows Domain

Verify the following:

- Make sure the user account has a password type of Open Directory.
- Make sure the workstation has joined the Windows domain of Mac OS X Server.

If a Windows User Has No Home Folder

If a user's home folder isn't mounted in Windows, verify the following:

- Make sure the correct home folder location is selected in the Home pane of Workgroup Manager.
- Make sure the home folder path is correct in the Windows pane of Workgroup Manager. It should be blank to use the home folder specified in the Home pane.
- Using Server Admin, connect to the server where the user's home folder resides. In the Servers list, select SMB, click Advanced, and then make sure "Enable virtual share points" is selected.
- If the drive letter chosen for the user conflicts with a drive letter that's in use on the Windows workstation, change the drive letter setting in the Windows pane of Workgroup Manager or the mappings of other drive letters on the workstation.

If a Windows User's Profile Settings Revert to Defaults

There are several reasons why a user's profile settings might revert to default:

- If the user profile location is not blank in the Windows pane of Workgroup Manager, the default share point for user profiles is not used. In this case, the user profile location must specify a valid SMB share point. Make sure the user profile location specifies an existing share point.

  For more information, see "Setting Up an SMB Share Point" on page 129.

- Make sure the home folder is specified correctly in the Windows and Home panes of Workgroup Manager. These panes should be configured in one of the following ways:
  - If the home folder path in the Windows pane is blank, make sure the correct home folder location is selected in the Home pane.
  - If the home folder path is not blank in the Windows pane, make sure the home folder path specifies a valid SMB share point.

- If the drive letter chosen for the user conflicts with a drive letter in use on the Windows workstation, change the drive letter setting in the Windows pane of Workgroup Manager or change the mappings of other drive letters on the workstation.

If a Windows User Loses the Contents of the My Documents Folder

Verify the following:

- Make sure the correct home folder location is selected in the Home pane of Workgroup Manager.
- Make sure the user profile path is correct in the Windows pane of Workgroup Manager. If the user profile path is blank, the default profile folder is used. The contents of My Documents are stored in the user profile.
- If the drive letter chosen for the user conflicts with a drive letter in use on the Windows workstation, change the drive letter setting in the Windows pane of Workgroup Manager or change the mappings of other drive letters on the workstation.

Solving Preference Management Problems

This section describes problems you might 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, check Workgroup Manager Help or consult the Apple Service & Support website (www.apple.com/support/).

Testing Your Managed Client Settings

If your managed computers use Mac OS X v10.5 or later, you can view managed settings in System Profiler on the computers.

Settings are organized by preference. For example, all managed Finder settings are listed in com.apple.finder.

To view managed client settings in System Profiler:

1. On a client computer, open System Profiler.
2. Open the Software disclosure triangle and then choose Managed Client.

If 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 might not be in a group or might be in only one group. Hold down the Option key during login to show the list of workgroups.

- The user's computer might not have its login preferences managed. In the Access pane of login preferences, select "Always show workgroup dialog during login." This preference is available for clients with Mac OS X v10.5 or later.

Your client computers must use Mac OS X v10.4 or later to select from workgroups. For more information about how to set login window access settings, see "Customizing the Workgroups Displayed at Login" on page 205.

If Users Can't Open Files

Ordinarily, when users double-click a file in the Finder or choose a file to open from the File menu in Finder, the related default application opens the file for them. If the user is in a managed environment, this method might 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 the user don't provide access to Preview, the file does not open. If the user has access to a different application that can handle PDF files, the user can open that application first and then open the file.

To make sure commonly used applications are available to users, groups, or lists of computers, use Workgroup Manager to add the application to the list of permitted applications in the Applications pane of Preferences.

For more information, see "Controlling User Access to Specific Applications and Folders" on page 176.

If Users Can't Add Printers to a Printer List

If you manage Printing preferences, you can allow users to add printers to the list of printers in Print & Fax System Preferences. In Printing preferences, select "Allow user to modify the printer list." If you don't select this, an administrator name and password is required to add or remove printers in Print & Fax System Preferences.

Note: When a user tries to print a document from an application, the printer the user added does not appear in the list of available printers. For more information, see "Preventing Users from Modifying the Printer List" on page 235.

You can also make printers available or unavailable to specific users, groups, or lists of computers by using the Printer List pane of Printing preferences. For more information, see "Making Printers Available to Users" on page 235.

If Login Items Added by a User Don't Open

In Workgroup Manager, you can use the Items pane of login preferences to specify items that open when a user logs in. The items that open at login are a combination of items specified for the user, the computer being used, and the group chosen at login.

If your management frequency setting is Always, when you select "User may add and remove additional items," a user can add additional login items. Selecting Always removes existing items from the user's login items list and replaces them with the items you list. It also prevents the user from disabling the items you list.

If your management frequency setting is Once, you can select "Merge with user's items," which causes one of the following:

- If the user has items in their login list (because he or she added them or they were added through preference management), merging only opens login items that appear on both the user's list and your list.
- If the user's login list does not include any items, all managed login items will open. If you do not select "Merge with user's items," all login items on either list will open. If you select Once, a user can remove any items added to their login list.

For details about managing automatically opened items, see "Automatically Opening Items After a User Logs In" on page 210.

If Items Placed in the Dock by a User Are Missing

In Workgroup Manager, you can use the Dock Items pane of Dock preferences to specify items that appear in a user's Dock. The set of items in a user's Dock is a combination of items specified for the user, the computer being used, and the group chosen at login.

If you deselect "Merge with user's Dock," all Dock items you place will override users' Dock items settings. Users can't add items to their Docks if you select Always and deselect "Merge with user's Dock."

If you select Always, users can't remove items from their Docks.

For more information about how to add Dock items, see "Adding Items to a User's Dock" on page 187.

If a User's Dock Has Duplicate Items

When you use Workgroup Manager to set up the same Dock item preferences for more than one account type (user, group, computer, or computer group), a managed user's Dock can contain duplicate items. For example, an application icon might appear more than once in the user's Dock.

Duplicate applications or folders work as expected when you open them. To correct duplicate Dock items, try removing Dock item preferences for all account types that affect the user, then carefully configure the Dock item preferences for the account types.

If Users See a Question Mark in the Dock

You can use Workgroup Manager to control the items a user sees in his or her Dock. Items in the Dock are aliases to original items stored elsewhere, such as on the computer's hard disk or on a remote server.

If you add items to a user's Dock that are not on the user's hard disk or other volume mounted on the user's computer, the items appear as question mark icons. Clicking these icons does not open the items.

If you add an item that is on the server and the user's computer, clicking the icon opens the item on the user's computer or mounted volume.

If Users See a Message About an Unexpected Error

When you manage Classic preferences and try to use the Extensions Manager, File Sharing, or Software Update control panels, you might 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 can't access the control panels mentioned above when Classic preferences are managed.

Users might also see this message if you select "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 not listed in the Items pane of the Applications preference in Workgroup Manager) in the Classic environment or in Mac OS X.

If You Can't Manage Network Views

Mac OS X Server v10.5 and later don't support managed network views.

To manage network views hosted on servers running Mac OS X Server v10.4, use the version of Workgroup Manager included with Mac OS X Server v10.4.

Importing and Exporting Account Information

Use Workgroup Manager to import and export accounts, or use the dsimport command-line tool to import accounts.

You can quickly import or export user, group, computer, and computer group accounts using Workgroup Manager. You can also use the `dsimport` command-line tool to import user and group accounts.

Understanding What You Can Import and Export

You can import all record types that are tracked in Workgroup Manager. Common record types include users, groups, computers, and computer groups. Starting with Mac OS X Server v10.4, you can import partial attributes of individual records, and combine attributes from different records.

When importing from custom files, the only attribute a record must have is a record name.

For a list of attributes, open Terminal and enter `man DirectoryServiceAttributes`. Alternately, if you have Xcode installed, you can view a list of attributes with improved formatting and more detailed descriptions by opening /System/Library/Frameworks/DirectoryService.framework/Headers/DirServicesConst.h.

You can't use an import file to change the following predefined users: daemon, root, nobody, unknown, or www. In addition, you can't use an import file to change the following predefined groups: admin, bin, daemon, dialer, mail, network, nobody, nogroup, operator, staff, sys, tty unknown, utmp, uucp, wheel, or www. However, you can add users to the wheel and admin groups.

You can use the `dsimport` tool to import records from a text-delimited file.

For descriptions of common record types and attributes, see *Open Directory Administration*. For a more complete list of attributes, enter `man DirectoryServiceAttributes`, or view the DirServicesConst.h file.

Limitations for Importing and Exporting Passwords

When creating or overwriting records, you must reset passwords for user accounts with Open Directory or shadow passwords. Importing passwords generally works if the password is a plain-text string in the import file.

Additionally, you must set the AuthMethod attribute so Workgroup Manager can import the password. You can't recover encrypted passwords in hash format in the import file.

You can't export passwords using Workgroup Manager or any other method. If you import user accounts from an export file, remember to manually set passwords or set default passwords to a known value.

Before exporting user accounts (or after importing them), you can set up a password policy that requires users to change their password at first login. For instructions on configuring password options, see "Choosing a Password Type and Setting Password Options" on page 78.

Maintaining GUIDs When Importing from Earlier Versions of Mac OS X Server

Globally unique identifiers (GUIDs) are used to verify user and group identity for ACL permissions and to manage user membership in groups and hierarchical groups. When you use Workgroup Manager or the `dsimport` tool to import users and groups created on versions of Mac OS X Server earlier than v10.4, GUIDs are automatically assigned.

After upgrading or migrating your server to Mac OS X Server v10.6, back up your accounts by exporting user and group accounts to ensure that all your accounts have GUIDs.

If you need to restore user or group accounts in the future, the generated export file enables you to import users and groups with their GUIDs (as well as file permissions and group memberships) intact.

If you lose user accounts and you then create new accounts with the same UID, GID, and short names as the lost accounts, the replacement accounts have new GUIDs assigned. A user's new GUID won't match the previous GUID, so the user won't retain prior ACL permissions or group memberships.

Similarly, if you import users or groups from a file that doesn't include the GUID attribute, Mac OS X Server assigns new GUIDs to every imported user and group.

To make sure that GUIDs and their relationship to specific users and groups remain the same if you need to reimport users and groups, create an export file using Mac OS X Server v10.6 and use this file instead of the export file created with an earlier server version.

Archiving the Open Directory Master

Instead of exporting and importing records as a backup of directory data, you can archive and restore the Open Directory master's directory and authentication data. By archiving a copy of the Open Directory master's directory, you can later restore the directory with passwords intact.

Using Workgroup Manager to Import Accounts

You can use Workgroup Manager to import user, group, computer, and computer group accounts into an Open Directory domain. When a file is imported, Workgroup Manager identifies the record format.

Before trying to import accounts using Workgroup Manager, create a character-delimited or XML file containing the accounts to import and place it in a location accessible by the computer from which you use Workgroup Manager.

An Open Directory domain supports files with up to 200,000 records.

Important: Workgroup Manager can only import files that use UNIX line breaks. When editing import files, use a text editor that supports UNIX line breaks.

You can also use the `dsimport` tool to import records from a text-delimited file. For more information, see "Using the Command Line to Import Accounts" on page 275.

For information about how to create a character-delimited file by hand or by using a database or spreadsheet application, see "Creating a Character-Delimited User Import File" on page 277.

To import accounts using Workgroup Manager:

1. In Workgroup Manager, click Accounts.
2. Make sure the directory services of the Mac OS X Server computer you're using are configured to access the directory domain.

   For instructions, see *Open Directory Administration*.
3. Click the globe icon and choose the domain where you want to import accounts.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Choose Server > Import and select an import file.
6. To indicate what to do when the short name of an account being imported matches that of an existing account, select one of the following Duplicate Handling options:
   - "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 has no value.
- "Append to existing record" appends data to existing data for a specific multivalue attribute in the existing account. Duplicates are not created. You can use this option when importing members into an existing group.
- "Don't check for duplicates" disables checking for duplicates, but it can cause misconfigured records and unexpected results. Make sure there are no duplicates before choosing this option. When you enable this option, it can decrease the time required to import.

7. To enable presets for a user or a group, select Preset for Users or Preset for Groups and choose presets from the two pop-up menus.

   If a setting is specified in the preset and an 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.

   For more information about how to create presets, see "Creating a Preset for User Accounts" on page 63 and "Creating a Preset for Group Accounts" on page 97.

8. In the First User ID field, enter a user ID for new user accounts without user IDs in the import file.

   New User IDs are then sequentially assigned for other accounts without listed user IDs.

9. In the Primary Group ID field, enter the group ID to assign to new user accounts for users that have no primary group ID in the import file.

10. Choose the level of detail for the log from the Logging Detail pop-up menu.

    Every time you import, a new log is created in ~/Library/Logs/ImportExport/.

11. Click Import.

Using the Command Line to Import Accounts

To import user and group accounts into a folder, use `dsimport`. The `dsimport` tool permits logging at three levels with the `-l` switch. You can also use the `dsimport` tool to import records from a flexible text–delimited file.

For more information, see the `dsimport` man page. For a list of record types and attributes, see *Open Directory Administration*. This also describes how to edit permitted attributes for each record type for use in an LDAP folder.

The `dsimport` tool is located in /usr/bin/.

For information about the formats of the files you can import, see "Creating a Character-Delimited User Import File" on page 277.

```
$ dsimport (-g|-s|-p) filepath DSNodePath (O|M|I|A|N) -u user -p password
     [options]
```

Parameter	Description
`-g|-s|-p`	Specify one of these to indicate the type of file you're importing: `-g` for a character-delimited file `-s` for an XML file exported from Users & Groups in Mac OS X Server v10.1.x `-p` for an XML file exported from AppleShare IP v6.x
`filepath`	Specify the path of the file to import.
`DSNodePath`	Specify the path to the Open Directory server node where the imported records will be added.
`O|M|I|A|N`	Use to specify how user data is handled if a record for an imported user exists in the folder: • `O`: Overwrite the matching record. • `M`: Merge the records. Empty attributes in the folder and assume values from the imported record. • `I`: Ignore imported record and leave the record unchanged. • `A`: Append data from an import record to an existing record. • `N`: Do not check for duplicates.
`user`	Specify the name of the Open Directory directory administrator.
`password`	Specify the password of the Open Directory directory administrator.
`options`	Use to specify additional command options. To see available options, execute the `dsimport` command with no parameters.

To import users and groups:

1. Create a file containing the accounts to import, and place it in a location accessible from the importing server.

   You can export this file from an earlier version of Mac OS X Server or AppleShare IP 6.3, or you can create a character-delimited file. See "Creating a Character-Delimited User Import File" on page 277.

   Open Directory supports up to 200,000 records.

2. Log in as the administrator of the directory domain you want to import accounts into.
3. Use the `dsimport` tool to import users and groups.

   For example, to import a file generated by Workgroup Manager named "sample" and export it into the LDAPv3 directory located at 192.168.2.2, use the following command:

```
$ dsimport -g sample /LDAPv3/192.168.2.2 -O -u diradmin
```

Replace *diradmin* with the short name of the directory administrator. When two records match, the import file overwrites the matching record.

4 To create home folders for imported users, use `createhomedir`.

See "Configuring Portable Computers" on page 151.

Creating a Character-Delimited User Import File

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. You can also create a character-delimited file manually by using a script, or by using a database or spreadsheet application.

The first record in the file, the record description, describes the format of each account record in the file. There are three options for the record description:

- 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 record description. A line in a character-delimited file that begins with # is ignored during importing.

Writing a Record Description

The record description specifies the fields in each record in the character-delimited file, specifies the delimiting characters, and specifies the escape character that precedes special characters in a record.

Encode the record description using the following elements in the order specified, separating them with a space:

- End-of-record indicator (in hex notation)
- Escape character (in hex notation)
- Field separator (in hex notation)
- Value separator (in hex notation)
- Type of accounts in the file (`dsRecTypeStandard:Users` or `dsRecTypeStandard:Groups`)
- Number of attributes in each account record
- List of attributes

For user accounts, the list of attributes must include the following, although you can omit UID and PrimaryGroupID if you specify a starting UID and a default primary group ID when you import the file:

- RecordName (the user's short name)

- Password
- UniqueID (the UID)
- PrimaryGroupID
- RealName (the user's full name)

In addition, you can include:

- UserShell (the default shell)
- NFSHomeDirectory (the path to the user's home folder)
- Other user data types, described in Open Directory Administration.

For group accounts, the list of attributes must include:

- RecordName (the group name)
- PrimaryGroupID (the group ID)
- GroupMembership

The following is an example of a record description:

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Users 7
RecordName Password UniqueID PrimaryGroupID
RealName NFSHomeDirectory UserShell
```

The following is an example of a record encoded using the previous description:

```
anne:Adl47E$:408:20:A. Johnsons, M.D.:/Network/Servers/somemac/Homes/
     anne:/bin/csh
```

The record consists of values, delimited by colons. Use a double-colon (::) to indicate that a value is missing.

The following is another example, which shows a record description and user records for users whose passwords are to be validated using Password Server. The record description should include a field named `dsAttrTypeStandard:AuthMethod`, and the value of this field for each record should be `dsAuthMethodStandard:dsAuthClearText`:

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Users 8
dsAttrTypeStandard:RecordName dsAttrTypeStandard:AuthMethod
dsAttrTypeStandard:Password dsAttrTypeStandard:UniqueID
dsAttrTypeStandard:PrimaryGroupID dsAttrTypeStandard:Comment
dsAttrTypeStandard:RealName dsAttrTypeStandard:UserShell
skater:dsAuthMethodStandard\:dsAuthClearText:pword1:374:11:comment:
Tony Hawk:/bin/csh
mattm:dsAuthMethodStandard\:dsAuthClearText:pword2:453:161::
Matt Mitchell:/bin/tcsh
```

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.

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
```

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 that the colon should not be treated as a delimiter. The backslash (\) is the escape character in this example. If the field separator is anything other than the colon, the escape character is not needed.

The method for setting an imported user's password type to Open Directory requires that the imported data has a password value. If the password value is missing for a user, the corresponding user record is created with a password type of Crypt or Shadow Password.

Before importing user accounts, remember to manually set passwords or set default passwords to a known value. After importing user records, you can set up a password policy that requires users to change their password at first login.

Note: Importing passwords generally works only if the password is a plain text string in the import file. Additionally, you need to set the AuthMethod attribute so that `dsimport` can import the password. Encrypted passwords that are in hash format in the import file cannot be recovered. Also, passwords cannot be exported using Workgroup Manager or any other method.

Using StandardUserRecord Shorthand

When the first record in a character-delimited import file contains `StandardUserRecord`, the following record description is assumed:

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Users 7
RecordName Password UniqueID PrimaryGroupID
RealName NFSHomeDirectory UserShell
```

An example user account looks like this:

```
anne:Adl47E$:408:20:A. Lo, M.D.:/Network/Servers/somemac/Homes/anne:/bin/
     csh
```

Using StandardGroupRecord Shorthand

When the first record in a character-delimited import file contains `StandardGroupRecord`, the following record description is assumed:

```
0x0A 0x5C 0x3A 0x2C dsRecTypeStandard:Groups 4
RecordName Password PrimaryGroupID GroupMembership
```

The following is an example of a record encoded using the description:

```
students:Ad147:88:johnson,miller,clark,chen,wong
```

Using Workgroup Manager to Export Accounts

You can use Workgroup Manager to export user, group, computer, and computer group accounts from an Open Directory domain into a character-delimited file that you can import into a different LDAP directory domain.

You can also use the `dsexport` tool to export records to a text-delimited file. For more information, see "Using the Command Line to Export Users and Groups" on page 280.

To export accounts using Workgroup Manager:

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

   For instructions, see *Open Directory Administration*.
3. Click the globe icon and then choose the domain where you want to import accounts.
4. To authenticate, click the lock and enter the name and password of a directory administrator.
5. Select the accounts to export.

   To choose multiple accounts to export, select the accounts while holding the Command or Shift key.
6. Choose Server > Export.
7. Specify the name to assign to the export file and where you want to create it.

   To browse to a location for storing the export file, click the disclosure triangle.
8. Click Export.

Using the Command Line to Export Users and Groups

To export records from Open Directory use `dsexport`.

The `dsexport` tool is in the /usr/bin/ folder.

```
$ dsexport filePath DSNodePath recordType options DSProxy
```

Parameter	Description
filepath	The name (including the path) of the file to export.
DSNodePath	The path to the Open Directory server node to export records from.
recordType	(Optional) The type of record to be exported from the Open Directory server node.
options	Additional command options. To see available options, execute the `dsexport` command with no parameters. Also, see the command's man page.
DSProxy	(Optional) A set of options for connecting to a proxy system. All options are needed. If you do not specify the password as an argument, the tool prompts you for it. Options are: `-a proxyAddress`: The address of the proxy machine the user wants to use. `-u proxyUser`: The username to use for the proxy connection. `-p proxyPassword`: The password to use for the proxy connection.

For example, use the following to export user records from the local Open Directory server node and store the exported data in the exportedUserRecords.out file:

```
$ dsexport exportedUserRecords.out /Local/Default dsRecTypeStandard:Users
```

Use the following to export group records for admin and staff from the LDAPv3 node on the proxy system (proxy.machine.com) to the exportedGroupRecords.out file:

```
$ dsexport exportedGroupRecords.out /LDAPv3/127.0.0.1
     dsRecTypeStandard:Groups -r admin, staff -a proxy.machine.com -u
     diradmin -p pass
```

Using XML Files Created with Mac OS X Server v10.1 or Earlier

You can use Server Admin in Mac OS X Server v10.1 or earlier to create an export file and import that file into an Open Directory domain using Workgroup Manager or `dsimport`.

The following user account attributes are exported into the XML files. An error occurs when you import a file with missing required attributes:

- Indication of whether user can log in
- Indication of whether user is a server administrator
- User ID (required)

- Primary group ID (required)
- Shell
- Comment
- Short name (required)
- Long name (required)
- Password format (required) and password text (required)
- Apple mail data
- ARA (Apple Remote Access—this data is ignored)

The following group account attributes might be present in XML files:

- Group name (required)
- Group ID (required)
- One member's short name (required)
- Other members' short names

Using XML Files Created with AppleShare IP 6.3

You can use the Web & File Admin application on an AppleShare IP 6.3 server to create an export file and then use Workgroup Manager or `dsimport` to import that file into an Open Directory domain.

The following user account attributes are exported into the XML files. An error occurs when you import a file with missing required attributes.

- Name (required, mapped to a long name)
- InetAlias (mapped to a short name)
- Comment
- Indication of whether user can log in
- Password format (required) and password text (required)
- Apple mail data
- An indicator for whether the user is a server administrator; the password change data; and an 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 subsequent imported account's user ID by one. It generates primary group IDs using the `-r` parameter.

When you import using Workgroup Manager, user IDs and primary group IDs are generated as you indicate in the dialog provided.

The following group account attributes might be present in these XML files:

- Group name (required)
- One member's short name (required)
- Other members' short names

The `dsimport` tool generates group IDs when you import this XML file, using the `-r` parameter to determine the group ID to start with, and incrementing each subsequent imported group's ID by one.

When you import using Workgroup Manager, group IDs are generated using the information you provide for group IDs in the import dialog.

Index

E

F

G

H

I

K

L

M

Q

R

S

T

U

V

W

X