Mac OS X Server
File Server Administration

For Version 10.6 Snow Leopard

Every effort has been made to ensure that the information in this manual is accurate. Apple Inc. is not responsible for printing or clerical errors.

Apple

1 Infinite Loop
Cupertino CA 95014-2084
www.apple.com

019-1411/2009-05-29

Contents

About This Guide

This guide describes how to configure and use file services with Mac OS X Server.

File sharing requires file server administrators to manage user privileges for shared folders and files. Configuring Mac OS X Server as a file server offers you reliable high-performance file sharing using native protocols for Mac, Windows, and Linux workgroups. The server fits seamlessly into any environment, including mixed-platform networks.

Mac OS X Server v10.6 delivers expanded functions of current features and introduces enhancements to support heterogeneous networks, maximize user productivity, and make file services more secure and easier to manage.

What's in This Guide

This guide includes the following sections:

- Chapter 1, "Understanding File Services," provides an overview of Mac OS X Server file services.
- Chapter 2, "Setting Up File Service Permissions," explains standard permissions and ACLs and discusses related security issues.
- Chapter 3, "Setting Up Share Points," describes how to share specific volumes and directories by using Apple Filing Protocol (AFP), Server Message Block (SMB)/ Common Internet File System (CIFS) protocol, File Transfer Protocol (FTP), and Network File System (NFS) protocol. It also describes how to set standard and ACL permissions.
- Chapter 4, "Working with AFP Service," describes how to set up and manage AFP service in Mac OS X Server.
- Chapter 5, "Working with SMB Service," describes how to set up and manage SMB service in Mac OS X Server.
- Chapter 6, "Working with NFS Service," describes how to set up and manage NFS service in Mac OS X Server.

- Chapter 7, "Working with FTP Service," describes how to set up and manage FTP service in Mac OS X Server.
- Chapter 8, "Solving Problems," lists potential solutions to common problems you might encounter while working with the file services in Mac OS X Server.

In addition, the Appendix , "Command Line Parameters for File Services," provides additional command-line parameters for file services .

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 Help Viewer while you're managing Mac OS X Server. You can view help on a server, or on an administrator computer. (An administrator computer is a Mac OS X computer with Mac OS X Server administrator software installed on it.)

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

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

  The onscreen help contains instructions taken from *Advanced Server Administration* and other administration guides.

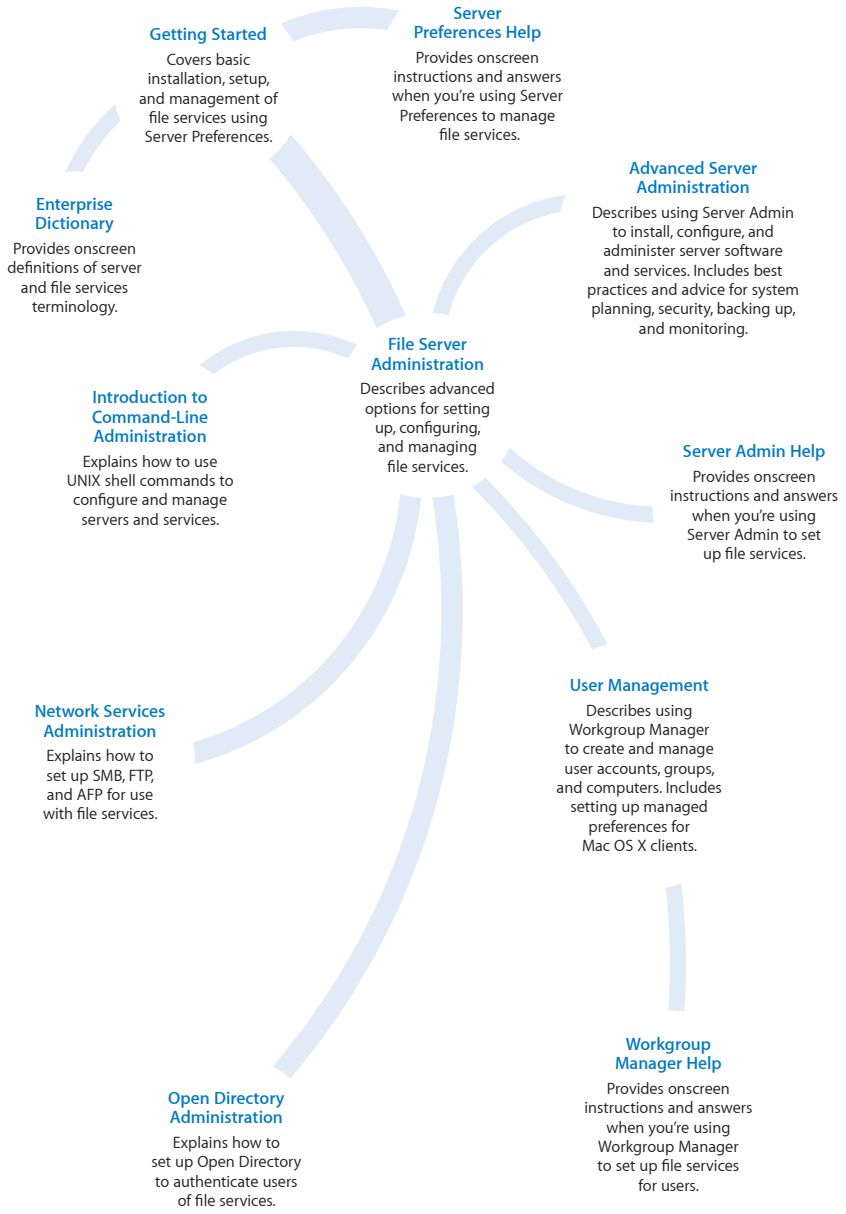
To see the most recent server help topics:

- 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 has a suite of guides that cover management of individual services. Each service may depend on other services for maximum utility. The documentation map below shows some related guides that you may need in order to fully configure file services to your specifications. You can get these guides in PDF format from the Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.


Getting Started
Covers basic installation, setup, and management of file services using Server Preferences.
Server Preferences Help
Provides onscreen instructions and answers when you're using Server Preferences to manage file services.
Enterprise Dictionary
Provides onscreen definitions of server and file services terminology.
Advanced Server Administration
Describes using Server Admin to install, configure, and administer server software and services. Includes best practices and advice for system planning, security, backing up, and monitoring.
File Server Administration
Describes advanced options for setting up, configuring, and managing file services.
Introduction to Command-Line Administration
Explains how to use UNIX shell commands to configure and manage servers and services.
Server Admin Help
Provides onscreen instructions and answers when you're using Server Admin to set up file services.
Network Services Administration
Explains how to set up SMB, FTP, and AFP for use with file services.
User Management
Describes using Workgroup Manager to create and manage user accounts, groups, and computers. Includes setting up managed preferences for Mac OS X clients.
Workgroup Manager Help
Provides onscreen instructions and answers when you're using Workgroup Manager to set up file services for users.
Open Directory Administration
Explains how to set up Open Directory to authenticate users of file services.

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 guide. 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 Resources website at 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 and go to:

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.
- *Apple Filing Protocol (AFP) website* (developer.apple.com/documentation/Networking/Conceptual/AFP)—manual describing AFP.
- *Samba website* (www.samba.org)—information about Samba, the open source software on which SMB service in Mac OS X Server are based.
- *Common Internet File System (CIFS) website* (www.ubiqx.org/cifs)—detailed description of how CIFS works.
- *File Transfer Protocol (FTP) website* (www.faqs.org/rfcs/rfc959.html)—home of the FTP Request for Comments (RFC) document.
- *File Transfer Protocol (TFTP) website* (asg.web.cmu.edu/rfc/rfc1350.html)—home of the TFTP RFC document.

Understanding File Services

1

Use this chapter to learn basic concepts regarding Mac OS X Server file services.

Mac OS X Server includes several file services that help you manage and maintain your shared network resources. Understanding each service and its associated protocol helps you determine how to plan and configure your network for optimum performance and security.

Protocol Overview

File services provide a way for client computers to access and share files, applications, and other resources on a network. Each file service uses a protocol to communicate between the server and client computers. Depending on your network configuration, you can choose from the following file services:

- AFP service uses Apple Filing Protocol (AFP) to share resources with clients who use Macintosh computers.
- SMB service uses the Server Message Block/Common Internet File System (SMB/CIFS) protocol to share resources with and provide name resolutions for clients who use Windows or Windows-compatible computers.
- FTP service uses File Transfer Protocol (FTP) to share files with anyone using FTP client software.
- NFS service uses the Network File System (NFS) protocol to share files and folders with users (typically UNIX users) who have NFS client software.

After configuring file services, you can manage shared network resources by monitoring network activity and controlling access to each service.

Protocol Security Comparison

When sharing network resources, configure your server to provide the necessary security.

AFP and SMB provide some level of encryption to secure password authentication. AFP and SMB do not encrypt data transmissions over the network so you should only use it on a securely configured network.

FTP does not provide password or data encryption. When using this protocol, make sure your network is securely configured. Instead of using FTP, consider using the `scp` or `sftp` command-line tools. These tools securely authenticate and securely transfer files.

The following table provides a comparison of the protocols and their authentication and encryption capabilities.

Protocol	Authentication	Data Encryption
AFP	Cleartext and encrypted (Kerberos) passwords.	Not encrypted. Data is visible during transmission.
NFS	Encrypted (Kerberos) password and system authentication.	Can be configured to encrypt all data transmission.
SMB	Cleartext and encrypted (NTLM v1, NTLM v2, LAN Manager, and Kerberos) passwords.	Not encrypted. Data is visible during transmission.
FTP	All passwords are sent as cleartext. No encryption.	Not Encrypted. Data is sent as cleartext.

Protocol Comparison

When sharing network resources, you might have more than one service turned on, depending on the platforms that require access to these resources. The following table describes which service protocols are supported for each platform.

Protocol	Platform	Default Ports
AFP	Mac OS X and Mac OS X Server	548
SMB	Mac OS X, Mac OS X Server, Windows, UNIX, and Linux	137, 138, and 139
FTP	Mac OS X, Mac OS X Server, Windows, UNIX, and Linux	21
NFS	Mac OS X, Mac OS X Server, Windows, UNIX, and Linux	2049

Deployment Planning

When planning your network, consider the protocols your network configuration requires. For example, if your network consists of multiplatform computers, consider using SMB and AFP services to permit access to both platforms.

Determining the Best Protocol for Your Needs

The file service protocols you use depend on your network configuration and what platforms you are supporting.

Determining Hardware Requirements for Your Needs

If you're sharing network resources with other networks over Ethernet, your firewall must permit communication through all ports associated with your service.

Planning for Outages and Failovers

When planning for outages and failovers, consider eliminating as many single points of failure on your network as possible. An example of a single point of failure is a single computer with a single hard disk and a single power source.

If you have a single computer, you can eliminate single points of failure by:

- Configuring your computer with more disk drives, using a redundant array of independent disks (RAID). By configuring a RAID you can help prevent data loss. For example, if the main disk fails, the system can still access data from other disk drives in the RAID.
- Connecting the power source of the computer to a backup power source.
- Providing another computer with the same configuration to eliminate the computer as the single point of failure. If you don't have another computer, you can configure your computer to reboot on power failure. This ensures your computer will reboot as soon as power is restored.

You can also help diminish the possibility of failure by ensuring that your equipment has proper operational conditions (for example, adequate temperature and humidity levels).

A more advanced method of eliminating a single point of failure involves link aggregation, load balancing, Open Directory replication, data backup, and using Xserve and RAID devices.

For more information about these topics, see *Xgrid Administration and High Performance Computing*.

Setting Up File Service Permissions 2

Use this chapter to learn about standard permissions, Access Control Lists (ACLs), and related security issues.

An important aspect of computer security is the granting and denying of permissions. A permission is the ability to perform a specific operation, such as gaining access to data or executing code. Permissions are granted at the level of folders, subfolders, files, or applications. Use Server Admin to set up file service permissions.

In this guide, the term *privileges* refers to the combination of ownership and permissions, while the term *permissions* refers to the permission settings that each user category can have (Read & Write, Read Only, Write Only, and None).

Permissions in the Mac OS X Environment

If you're new to Mac OS X and are not familiar with UNIX, there are differences in the way ownership and permissions are handled compared to Windows.

To increase security and reliability, Mac OS X sets many system folders, such as /Library/, to be owned by the root user (literally, a user named *root*). Files and folders owned by root can't be changed or deleted by you unless you're logged in as root.

Be careful—there are few restrictions on what you can do when you log in as root, and changing system data can cause problems. An alternative to logging in as root is to use the `sudo` command.

Note: The Finder calls the root user *system*.

By default, files and folders are owned by the user who creates them. After they're created, items keep their privileges (a combination of ownership and permissions) even when moved, unless the privileges are explicitly changed by their owners or an administrator.

Therefore, new files and folders you create are not accessible by users if they are created in a folder that users don't have privileges for. When setting up share points, make sure that items have the correct access privileges for the users you want to share them with.

Kinds of Permissions

Mac OS X Server supports two kinds of file and folder permissions:

- Standard Portable Operating System Interface (POSIX) permissions
- Access Control Lists (ACLs)

Standard POSIX permissions enable you to control access to files and folders based on three categories of users: Owner, Group, and Others. Although these permissions give you adequate control over who can access a file or a folder, they lack the flexibility and granularity that many organizations require to deal with elaborate user environments.

This is where ACLs come in handy. An ACL provides an extended set of permissions for a file or folder and enables you to set multiple users and groups as owners. In addition, ACLs are compatible with Windows Server 2003 and Windows XP, giving you added flexibility in a multiplatform environment.

Standard Permissions

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

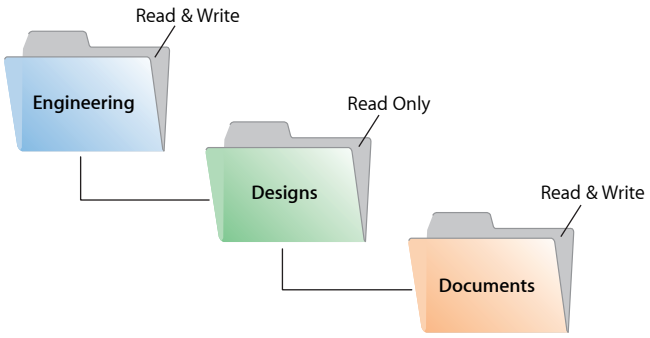
Users can	Read & Write	Read Only	Write Only	None
Open a shared file	Yes	Yes	No	No
Copy a shared file	Yes	Yes	No	No
Open a shared folder or share point	Yes	Yes	No	No
Copy a shared folder or share point	Yes	Yes	No	No
Edit a shared file	Yes	No	No	No
Move items to a shared folder or share point	Yes	No	Yes	No
Move items from a shared folder or share point	Yes	No	No	No

Note: QuickTime Streaming Server (QTSS) and WebDAV have separate permissions settings. For information about QTSS, and *Web Technologies Administration.* see the QTSS online help, QuickTime website (www.apple.com/quicktime/products/qtss) and *QuickTime Streaming and Broadcasting Administration*. You'll find information about Web permissions in *Web Technologies Administration.*

Explicit Permissions

Share points and the shared items they contain (including folders and files) have separate permissions. If you move an item to a different folder, it retains its permissions and doesn't adopt the permissions of the folder where you moved it.

In the following illustration, the second folder (Designs) and the third folder (Documents) were assigned permissions that are different from those of their parent folders:



When ACLs are not enabled, you can also set up an AFP or SMB share point so new files and folders inherit the permissions of their parent folder. See "Changing AFP Settings for a Share Point" on page 39 or "Changing SMB Settings for a Share Point" on page 40.

The User Categories Owner, Group, and Others

You can assign standard POSIX access permissions separately to three categories of users:

- **Owner**—A user who creates an item (file or folder) on the file server is its owner and automatically has Read & Write permissions for that folder. By default, the owner of an item and the server administrator are the only users who can change its access privileges (but you can enable a group or others to use the item). The administrator can also transfer ownership of the shared item to another user.

  Note: When you copy an item to a drop box on an Apple file server, ownership of the item doesn't change. Only the owner of the drop box or root has access to its contents.

- **Group**—You can put users who need the same access to files and folders in group accounts. Only one group can be assigned access permissions to a shared item. For more information about creating groups, see *User Management*.
- **Others**—Others is any user (registered user or guest) who can log in to the file server.

Hierarchy of Permissions

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

- Group permissions override Others permissions.
- Owner permissions override Group permissions.

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

The more restrictive permissions always take precedence. For example, if a user belongs to a group that has No Access assigned to an item while the Others permissions are set to Read & Write access, the item with a No Access privilege overrides the Others setting, denying the user access to the item.

Client Users and Permissions

Users of AppleShare Client software can set access privileges for files and folders they own. Users who use Windows file sharing services can also set access privileges.

Standard Permission Propagation

Server Admin lets you specify which standard permissions to propagate. For example, you can propagate only the permission for Others to all descendants of a folder and leave the permissions for Owner and Group unchanged. For more information, see "Propagating Permissions" on page 55.

ACLs

When standard POSIX permissions are not enough, use access control lists (ACLs). 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.

ACLs in Mac OS X Server enable you to set file and folder access permissions to multiple users and groups in addition to standard POSIX permissions. This makes it easy to set up collaborative environments with smooth file sharing and uninterrupted workflows, without compromising security.

ACLs provide an extended set of permissions for a file or folder to give you more granularity when assigning privileges than standard permissions would provide. For example, rather than giving a user full writing permissions, you can restrict him or her to create only folders and not files.

Apple's ACL model supports 13 permissions for controlling access to files and folders, as described in the following table.

Permission name	Type	Description
Change Permissions	Administration	User can change standard permissions.
Take Ownership	Administration	User can change the file's or folder's ownership to himself or herself.
Read Attributes	Read	User can view the file's or folder's attributes (for example, name, date, and size).
Read Extended Attributes	Read	User can view the file's or folder's attributes added by third-party developers.
List Folder Contents (Read Data)	Read	User can list folder contents and read files.
Traverse Folder (Execute File)	Read	User can open subfolders and run a program.
Read Permissions	Read	User can view the file's or folder's standard permissions using the Get Info or Terminal commands.
Write Attributes	Write	User can change the file's or folder's standard attributes.
Write Extended Attributes	Write	User can change the file's or folder's other attributes.
Create Files (Write Data)	Write	User can create files and change files.
Create Folder (Append Data)	Write	User can create subfolders and add data to files.
Delete	Write	User can delete file or folder.
Delete Subfolders and Files	Write	User can delete subfolders and files.

In addition to these permissions, the Apple ACL model defines four types of inheritance that specify how these permissions are propagated:

- *Apply to this folder:* Apply (Administration, Read, and Write) permissions to this folder.
- *Apply to child folders:* Apply permissions to subfolders.
- *Apply to child files:* Apply permissions to the files in this folder.

- *Apply to all descendants:* Apply permissions to descendants. To learn how this option works with the previous two, see "To see the most recent server help topics:" on page 10.

The ACL Use Model

The ACL use model focuses on access control at the folder level, with most ACLs applied to files as the result of inheritance.

Folder-level control determines which users have access to the contents of a folder. Inheritance determines how a defined set of permissions and rules pass from the container to the objects in it.

Without use of this model, administration of access control would quickly become a nightmare: you would need to create and manage ACLs on thousands or millions of files.

In addition, controlling access to files through inheritance frees applications from maintaining extended attributes or explicit ACEs when saving a file because the system applies inherited ACEs to files. For information about explicit ACEs, see "To get the most recent onscreen help for Mac OS X Server:" on page 10.

ACLs and Standard Permissions

You can set ACL permissions for files and folders in addition to standard permissions. For more information about how Mac OS X Server uses ACL and standard permissions to determine what users can and cannot do to a file or folder, see "Rules of Precedence" on page 26.

ACL Management

In Mac OS X Server, you create and manage ACLs in the Permissions pane of File Sharing in Server Admin. The Get Info window in Finder displays the logged-in user's effective permissions. For information about setting up and managing ACLs, see "Setting ACL Permissions" on page 38 and "Managing Share Point Access Privileges" on page 50.

In addition to using Server Admin to set and view ACL permissions, you can also use the `ls` and `chmod` command-line tools. For more information, see the corresponding man pages and *Introduction to Command-Line Administration*.

You define ACLs for share points, files, and folders using Server Admin.

Supported Volume Formats and Protocols

Only HFS+ provides local file system support for ACLs. In addition, only SMB and AFP provide network file system support for ACLs in Windows and Apple networks respectively.

Access Control Entries (ACEs)

An ACE is an entry in an ACL that specifies, for a group or a user, access permissions to a file or folder, and the rules of inheritance.

What's Stored in an ACE

An ACE contains the following fields:

- **User or Group.** An ACE stores a universally unique ID for a group or user, which permits unambiguous resolution of identity.
- **Type.** An ACE supports two permission types, Allow and Deny, which determine whether permissions are granted or denied in Server Admin.
- **Permission.** This field stores the settings for the 13 permissions supported by the Apple ACL model.
- **Inherited.** This field specifies whether the ACE is inherited from the parent folder.
- **Applies To.** This field specifies what the ACE permission is for.

Explicit and Inherited ACEs

Server Admin supports two types of ACEs:

- Explicit ACEs, which are those you create in an ACL. See "Adding ACEs to ACLs" on page 51.
- Inherited ACEs, which are ACEs you created for a parent folder that were inherited by a descendant file or folder.

Note: Inherited ACEs cannot be edited unless you make them explicit. Server Admin enables you to convert an inherited ACE to an explicit ACE. For more information, see "Changing Inherited ACEs for a Folder to Explicit" on page 54.

Understanding Inheritance

ACL inheritance lets you determine how permissions pass from a folder to its descendants.

The Apple ACL Inheritance Model

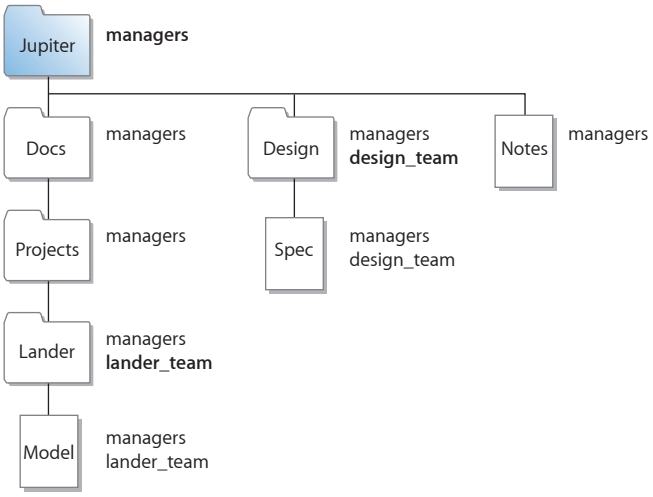
The Apple ACL inheritance model defines four options that you select or deselect in Server Admin to control the application of ACEs (in other words, how to propagate permissions through a folder hierarchy):

Inheritance option	Description
Apply to this folder	Apply (Administration, Read, and Write) permissions to this folder
Apply to child folders	Apply permissions to subfolders
Apply to child files	Apply permissions to the files in this folder
Apply to all descendants	Apply permissions to all descendants. ***Note:*** If you want an ACE to apply to all descendants without exception, you must select the "Apply to child folders" and "Apply to child files" options in addition to this option. For more information, see "ACL Inheritance Combination" on page 25.

Mac OS X Server propagates ACL permissions at two well-defined times:

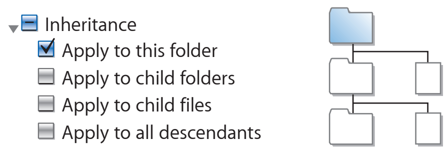
- By the kernel at file or folder creation time—when you create a file or folder, the kernel determines what permissions the file or folder inherits from its parent folder.
- When initiated by administrator tools—for example, when using the Propagate Permissions option in Server Admin.

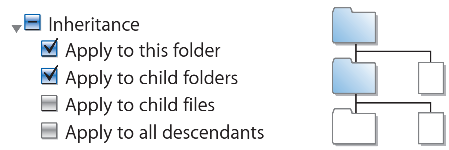
The following figure shows how Server Admin propagates two ACEs (managers and design_team) after ACE creation. Bold text represents an explicit ACE and regular text an inherited ACE.

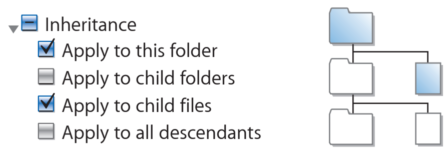


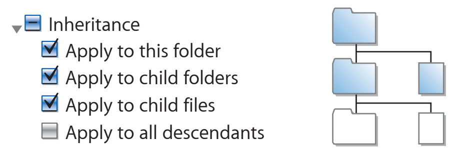
ACL Inheritance Combination

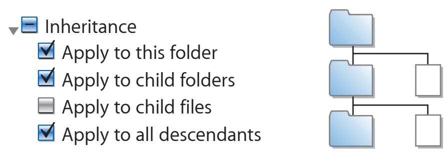
When you set inheritance options for an ACE in Server Admin, you can choose from 12 unique inheritance combinations for propagating ACL permissions.

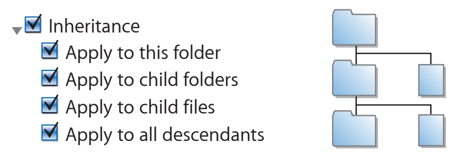


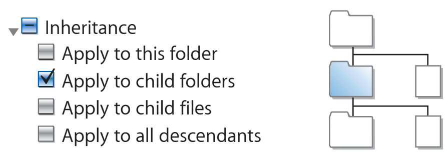


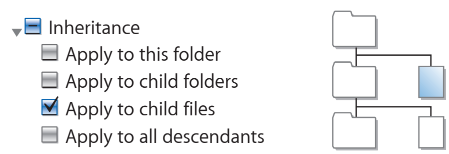


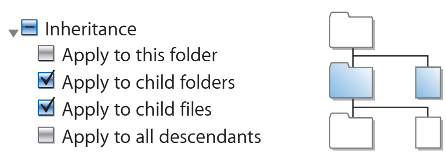


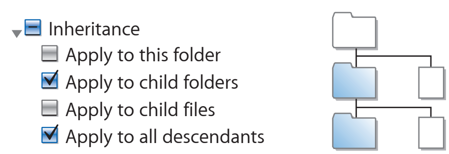


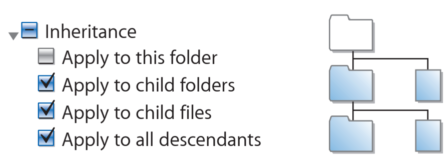


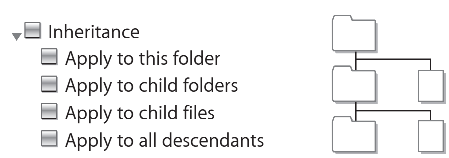










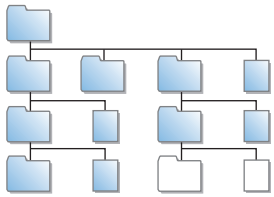


ACL Permission Propagation

Server Admin provides a feature that lets you force the propagation of ACLs. Although this is done automatically by Server Admin, there are cases when you might want to manually propagate permissions:

- You can propagate permissions to handle exceptions. For example, you might want ACLs to apply to all descendants except for a subtree of your folder hierarchy. In this case, you define ACEs for the root folder and set them to propagate to descendants. Then, you select the root folder of the subtree and propagate permissions to remove the ACLs from descendants of that subtree.

  In the following example, the items in white had their ACLs removed by manually propagating ACLs.



- You can propagate permissions to reapply inheritance in cases where you removed a folder's ACLs and decided to reapply them.
- You can propagate permissions to clear all ACLs at once instead of going through a folder hierarchy and manually removing ACEs.
- When you propagate permissions, the permissions of bundles and root-owned files and folders are not changed.

For more information about how to manually propagate permissions, see "Propagating Permissions" on page 55.

Rules of Precedence

Mac OS X Server uses the following rules to control access to files and folders:

- **Without ACEs, POSIX permissions apply.** If a file or folder has no ACEs defined for it, Mac OS X Server applies standard POSIX permissions.
- **With ACEs, order is important.** If a file or folder has ACEs defined for it, Mac OS X Server starts with the first ACE in the ACL and works its way down the list until the requested permission is satisfied or denied.

  You can change the ACE order from the command line using the `chmod` command.
- **Allow permissions are cumulative.** When evaluating Allow permissions for a user in an ACL, Mac OS X Server defines the user's permissions as the union of all permissions assigned to the user, including standard POSIX permissions.

After evaluating ACEs, Mac OS X Server evaluates the standard POSIX permissions defined for the file or folder. Then, based on the evaluation of ACL and standard POSIX permissions, Mac OS X Server determines the type of access a user has to a shared file or folder.

Tips and Advice

Mac OS X Server combines traditional POSIX permissions with ACLs. This combination provides great flexibility and a fine level of granularity in controlling access to files and folders. However, if you're not careful in how you assign privileges, it'll be very hard for you to keep track of how permissions are assigned.

With 17 permissions, you can choose from a staggering 98,304 combinations. Add to that a sophisticated folder hierarchy, many users and groups, and many exceptions, and you have a recipe for considerable confusion.

This section offers useful tips and advice to help you get the most out of access control in Mac OS X Server and avoid the pitfalls.

Manage Permissions at the Group Level

Assign permissions to groups first, and assign permissions to individual users only when there is an exception.

For example, you can assign all teachers in a school district Read and Write permissions to a specific share point, but deny Anne Johnson, a temporary teacher, permission to read a specific folder in the share point's folder hierarchy.

Using groups is the most efficient way of assigning permissions. After creating groups and assigning them permissions, you can add and remove users from groups without reassigning permissions.

Gradually Add Permissions

Assign only necessary permissions and then add permissions only when needed. As long as you're using Allow permissions, Mac OS X Server combines the permissions.

For example, you can assign the Students group partial reading permissions on an entire share point. Then, where needed in the folder hierarchy, you can give the group more reading and writing permissions.

Use the Deny Rule Only When Necessary

When Mac OS X Server encounters a Deny permission, it stops evaluating other permissions the user might have for a file or folder and applies the Deny permission. Therefore, use Deny permissions only when absolutely necessary. Keep a record of these Deny permissions so you can delete them when they are not needed.

Always Propagate Permissions

Inheritance is a powerful feature, so take advantage of it. By propagating permissions down a folder hierarchy, you save yourself the time and effort required to manually assign permissions to descendants.

Use the Effective Permission Inspector

Frequently use the Effective Permission Inspector to make sure users have the correct access to important resources. This is especially important after changing ACLs. Sometimes, you might inadvertently give someone more or fewer permissions than needed. The inspector helps you detect these cases.

For more information about the inspector, see "Determining a User's File or Folder Permissions" on page 56.

Protect Applications from Being Modified

If you are sharing applications, make sure you set permissions for applications so that no one, except a trusted few, can change them. This is a vulnerability that attackers can exploit to introduce viruses or Trojan horses in your environment.

Keep It Simple

You can unnecessarily complicate file access management if you're not careful. Keep it simple. If standard POSIX permissions do the job, use those, but if you must use ACLs, avoid customizing permissions unless you need to.

Also, use simple folder hierarchies when feasible. A little strategic planning can help you create effective and manageable shared hierarchies.

Common Folder Configurations

When sharing files and folders between computers, you can set custom permissions to grant or restrict access to those files and folders.

Before you begin setting custom file and folder permissions, you might want to investigate how the file and folder will be shared, who has access, and what type of access you want users to have. A recommended way to manage file and folder permissions is to create groups of users who share the same privileges.

Depending on your network environment you can use either POSIX, ACL, or both to manage file or folder access.

The following table shows examples of the POSIX permissions and the ACL permissions necessary to configure some common folder sharing settings.

Folder	ACL (Everyone)	POSIX
Drop box	Permission Type: Allow Select the following checkboxes: • Traverse Folder • Create Files • Create Folder • All inheritance options	Owner: read, write, execute Group: read, write, execute Other: write Example: drwxrwx-w- Set the owner to root or localadmin and set the group to admin.
Backup share	Permission Type: Allow Select the following checkboxes: • List Folder Contents • Create Files • Create Folder	Owner: read, write, execute Group: read, write, execute Other: no permissions Example: drwxrwx--- Set the owner to root and set the group to admin.
Home folder	Permission Type: Deny • Delete • Apply to this folder • Apply to all descendants	Owner: read, write, execute Group: read only Other: read only Example: drwxr--r--

File Services Access Control

Server Admin in Mac OS X Server enables you to configure service access control lists (SACLs), which enable you to specify which users and groups have access to AFP, FTP, and SMB file services.

Using SACLs enables you to add another layer of access control on top of standard POSIX and ACL permissions. Only users and groups listed in an SACL have access to its corresponding service. For example, to prevent users from accessing a server's AFP share points, including home folders, remove the users from the AFP service's SACL.

For information about restricting access to file services using SACLs, see "Setting SACL Permissions" on page 66.

Customizing Shared Network Resources

The Network folder (/Network/) contains shared network resources. The Network folder is accessible in the Finder sidebar either under Devices > Computer > Network or Shared > All. You can customize the contents of the Network folder for client computers by setting up automatically mounting share points.

Share Points in the Network Folder

By default, the Network folder contains at least these subfolders:

- Applications
- Library
- Servers

You can mount share points in any of these subfolders. For more information, see "Automatically Mounting Share Points for Clients" on page 46.

More servers and shared items are added as they are discovered on your network.

Adding System Resources to the Network Library Folder

The Library folder, located in /Network/, is included in the system search path. This gives you the ability to make any type of system resource (usually found in the local Library folder) available on the network. These resources could include fonts, application preferences, ColorSync profiles, desktop pictures, and so forth.

You can use this capability to customize your managed client environment.

For example, suppose you want a specific set of fonts to be available to each user in an Open Directory domain. You would create a share point containing the fonts and then set the share point to mount automatically as a shared library on client computers in /Network/Library/Fonts/. For more information, see "Automatically Mounting Share Points for Clients" on page 46.

Security Considerations

The most effective method of securing your network is to assign correct privileges for each file, folder, and share point you create.

Restricting Access to File Services

As stated in "File Services Access Control" on page 29, you can use Service Access Control Lists (SACLs) to restrict access to AFP, FTP, and SMB services.

Restricting Access to Everyone

Be careful when creating and granting access to share points, especially if you're connected to the Internet. Granting access to Everyone (or to World in NFS) could expose your data to anyone on the Internet. For NFS, it is recommended that you do not export volumes to World and that you use Kerberos to provide security of NFS volumes.

Restricting Access to NFS Share Points

NFS share points without the use of Kerberos don't have the same level of security as AFP and SMB, which require user authentication (entering a user name and password) to gain access to a share point's contents.

If you have NFS clients, you might want to set up a share point to be used only by NFS users or configure NFS with Kerberos. NFS doesn't support SACLs. For more information, see "Protocol Security Comparison" on page 14.

Restricting Guest Access

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

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, take the following precautions by using File Sharing in Server Admin:

- Depending on the controls you want to place on guest access to a share point, consider the following options:
  - Set privileges for Everyone to None for files and folders that guest users shouldn't access. Items with this privilege setting can be accessed only by the item's owner or group.
  - Put all files available to guests in one folder or set of folders and then assign the Read Only privilege to the Everyone category for that folder and each file in it.
  - Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder.
- Don't export NFS volumes to World. Restrict NFS exports to a subnet or a specific list of computers.
- Disable access to guests or anonymous users over AFP, FTP, and SMB using Server Admin.
- Share individual folders instead of entire volumes. The folders should contain only those items you want to share.

Setting Up Share Points

3

Use this chapter to learn how to share specific volumes and directories by using AFP, SMB, FTP, and NFS, and to set standard and ACL permissions.

You use File Sharing in Server Admin to share information with clients of Mac OS X Server and to control access to shared information by assigning access privileges.

To share folders or volumes on the server, set up share points. A share point is a folder, hard disk, hard disk partition, CD, or DVD whose files are available for access across a network. It's the point of access at the top level of a hierarchy of shared items.

Users with access privileges to share points see them as volumes mounted on their desktops or in their Finder windows.

Share Points and the Mac OS X Network Folder

If you configure your computer to connect to LDAP directory domains and you set it with specific data mappings, you can control the access and availability of network services by using Server Admin to:

- Identify share points and shared domains that you want to mount automatically in a user's /Network/Servers/ folder, accessible in the Finder sidebar either under Devices > Computer > Network, or Shared > All.
- Add user records and group records (as defined in Workgroup Manager) and configure their access.

When configuring share points, you must define the users or groups that will access the share points. You can use Workgroup Manager to:

- Define user and group records and configure their settings.
- Define lists of computers that have the same preference settings and that are available to the same users and groups.

For information about configuring users and groups, see *User Management*.

Automounting

You can configure client computers to automatically mount share points. These share points can be static or dynamic:

- **Static share points** are mounted on demand. You can assign statically mounted share points to specific folders.
- **Dynamic share points** are mounted on demand and are in the /Network/Servers/*server_name/* folder.

Share Points and Network Home Folders

Network authenticated users can have their home folder stored locally on the client computer they are using or on a network server. Network home folders are an extension of simple automounts.

A home folder share point is mounted when the user logs in. It provides the user the same environment to store files as if the folders were on the local computer.

The benefit of network home folders is that they can be accessed by any client computer that logs in to a specific server that provides network home folder services for that user.

For information, see "Network Home Folders" on page 35.

Setup Overview

You use File Sharing in Server Admin to create share points and set privileges for them.

Here is an overview of the basic steps for setting up share points:

Step 1: Read "Before Setting Up a Share Point" For issues to consider before sharing information about your network, read "Before Setting Up a Share Point" on page 34.

Step 2: Locate or create the information you want to share Decide which volumes, partitions, or folders you want to share.

You might want to move folders and files to different locations before setting up the share point. You might also want to partition a disk into volumes so you can give each volume different access privileges or create folders that have different levels of access.

See "Shared Information Organization" on page 35.

Step 3: Set up share points and set privileges When you designate an item to be a share point, you also set its privileges. You create share points and set privileges using File Sharing in Server Admin. See "Setting Up a Share Point" on page 36.

Step 4: Turn specific file services on For users to access share points, you must turn on the required Mac OS X Server file services. For example, if you use AFP with your share point, you must turn on AFP service. You can share an item using more than one protocol.

For more information, see Chapter 5, "Working with SMB Service"; Chapter 6, "Working with NFS Service"; or Chapter 7, "Working with FTP Service."

Before Setting Up a Share Point

Before you set up a share point, consider the following topics:

- Client privileges
- File sharing protocols
- Shared information organization
- Security
- Network home folders
- Disk quotas

Client Privileges

Before you set up a share point, you should understand how privileges for shared items work. Determine which users need access to shared items and what permissions you want those users to have. Permissions are described in Chapter 2. See "Kinds of Permissions" on page 18.

File Sharing Protocols

You also must know which protocols clients use to access the share points. In general, you should set up unique share points for each type of client and share them using a single protocol:

- Mac OS clients—Apple Filing Protocol (AFP)
- Windows clients—Server Message Block (SMB)
- UNIX clients—Network File System (NFS)
- FTP clients—File Transfer Protocol (FTP)

Note: With unified locking, applications can use locks to coordinate access to files even when using different protocols. This permits users working on multiple platforms to share files across AFP, SMB, and NFS protocols without worrying about file corruption caused by locking issues between protocols.

In some cases you might want to share an item using more than one protocol. For example, Mac OS and Windows users might want to share graphics or word processing files that either file protocol can use. If so, you can create a single share point that supports both platforms.

Conversely, you might want to set up share points that support a single protocol even though you have different kinds of clients.

For example, if most of your clients are UNIX users and only a few are Mac OS clients, you might want to share items using only NFS to keep your setup simple. However, NFS doesn't provide AFP features that Mac OS users are accustomed to, such as Spotlight searching, native ACL, and extended attribute support.

Also, if you share applications or documents that are exclusively for Windows users, you can set up an SMB share point to be used only by them. This provides a single point of access for Windows users and lets them take advantage of opportunistic and strict file locking. For more information about file locking, see "File Locking with SMB Share Points" on page 94.

Note: If you enable AFP and SMB services on your server, Mac OS clients can connect to the server over AFP or SMB. If Windows users want to connect to your server over AFP, they must use third-party AFP client software.

Shared Information Organization

Organize shared information before you set up the share points, especially if you're setting up network home folders.

After you create share points, users form mental maps of the organization of the share points and the items they contain. Changing share points and moving information around can cause confusion.

Security

Review the issues discussed in "Security Considerations" on page 30.

Network Home Folders

If you're setting up a share point on your server to store user home folders, keep these points in mind:

- The /Users share point is set up by default to be used for storing home folders when you install Mac OS X Server. You can use this preconfigured share point for user home folders or you can create one on a local volume.
- The Automount settings for the share point should indicate that it's used for user home folders.
- The share point should be in the same Open Directory domain where user accounts are defined.
- To provide service to all types of clients, the complete pathname of an AFP or NFS network home folder must not contain spaces and must not exceed 89 characters. For more information, see Apple Knowledge Base article 107695 at docs.info.apple.com/article.html?artnum=107695.

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 the related 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.

For more information about configuring disk quotas for users and groups, see "Configuring Share Point Quotas" on page 64.

Setting Up a Share Point

This section describes how to create share points and set share point access privileges. It also describes how to share using specific protocols (AFP, SMB, FTP, or NFS) and how to automatically mount share points on client desktops.

For more tasks that you might perform after you set up sharing on your server, see "Managing Share Points" on page 47.

Creating a Share Point

You use File Sharing in Server Admin to share volumes (including disks, CDs, and DVDs), partitions, and individual folders by setting up share points.

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 a share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Volumes to list the available volumes to share.

To create a share point of an entire volume, select the volume from the list.

To share a folder within a volume, select the volume in the list and click Browse to locate and select the folder.

4 Click Share.

If you must create a folder for your share point, click Browse, click New Folder, enter the name of the folder, and click Create.

5 Click Save.

By default, the new share point is shared using AFP and SMB, but not FTP and NFS.

To configure your share point for a specific protocol or to export the share point using NFS, click Protocol Options and choose the protocol. Settings specific to each protocol are described in the following sections.

From the command line:

- To create a share point:

```
$ sudo sharing -a path -s shareflags
```

Parameter	Description
path	The full path to the folder you want to share.
shareflags	A three-digit binary number indicating the protocols used to share the folder. The digits represent, from left to right, AFP, FTP, and SMB. `1`=shared, `0`=not shared.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Setting Privileges

Mac OS X Server provides two methods of access control to files and folders: Standard permissions and ACL permissions. These methods are described in the following sections.

Setting Standard Permissions

When you don't need the flexibility and granularity that access control lists (ACLs) provide, or in cases where ACLs are not supported, use standard POSIX permissions (Read & Write, Read Only, Write Only, and None) to control access to a share point and its contents.

To set standard permissions on a share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Permissions below the list.
5. To set the owner or group of the shared item, enter names or drag names from the Users & Groups window to the owner or group records in the permissions table.

   Owner and group records are listed under the POSIX heading. The owner record is the one with the single user icon and the group record is the one with the group icon.

   To open the Users & Groups window, click Add (+). If you don't see a recently created user or group, click the Refresh button (below the Servers list).

   You can also edit POSIX owner and group names by double-clicking the relevant permissions record and dragging a name from the Users & Groups window into the User/Group field. Or you can enter a name in the User/Group field in the window that appears.

   To change the autorefresh interval, choose Server Admin > Preferences and change the value of the "Auto-refresh status every" field.
6. To change the permissions for the Owner, Group, and Others, use the arrows in the Permission column to access the Permission pop-up menu in the relevant row of the permissions table.

   Others is any user that logs in to the file server who is not the owner and does not belong to the group.
7. Click Save.

   The new share point is shared using AFP and SMB, but not FTP and NFS.

Setting ACL Permissions

To configure ACL permissions for a share point or folder, you create a list of access control entries (ACEs).

For each ACE, you can set 17 permissions with Allow, Deny, and Static inheritance, so you have fine-grain control over access permissions, something that you don't have when using standard permissions. For example, you can separate delete permissions from write permissions so that a user can edit a file but cannot delete it.

To set ACL permissions on a share point or a folder:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.

4 Click Permissions below the list.

5 Open the Users & Groups window by clicking Add (+).

6 Drag groups and users from the Users & Groups window into the ACL Permissions list to create ACEs.

By default, each new ACE gives the user or group full read and inheritance permissions. To change ACE settings, see "Editing ACEs" on page 52.

The first entry in the list takes precedence over the second, which takes precedence over the third, and so on. For example, if the first entry denies a user the right to edit a file, other ACEs that allow the same user editing permissions are ignored. In addition, the ACEs in the ACL take precedence over standard POSIX permissions.

For more information about permissions, see "Rules of Precedence" on page 26.

7 To set the relevant permissions, use the arrows in the column fields for each entry in the list.

The ACE order in the list changes depending on the level of access when the permissions are saved.

8 Click Save.

Changing AFP Settings for a Share Point

You can use Server Admin to choose whether a share point is available through AFP and to change settings such as the share point name that AFP clients see and whether guest access is permitted.

The default settings for a new share point should make it readily accessible to Mac OS 8, Mac OS 9, and Mac OS X clients.

To change the settings of an AFP share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point from the list.

4 Click Share Point below the list.

5 Click Protocol Options.

This opens the protocol window with configuration options for AFP, SMB, FTP, and NFS.

6 Click AFP.

7 Provide AFP access to the share point by selecting "Share this item using AFP."

8 Permit unregistered users to access the share point by selecting "Allow AFP guest access."

For greater security, don't select this item.

9 To change the name that clients see when they browse for and connect to the share point using AFP, enter a name in the "Custom AFP name" field.

Changing the custom AFP name does not affect the name of the share point itself, only the name that AFP clients see.

10 Click OK, then click Save.

From the command line:

- To change AFP settings:

```
$ sudo sharing -e path -s 100 -A customname -g guestflags
```

Parameter	Description
path	The full path to the share point.
customname	The name of the share point. If you don't specify the custom name, it's set to the name of the folder, the last name in `path`.
guestflags	A group of flags indicating which protocols allow guest access. The flags are written as a three-digit binary number with the digits representing, from left to right, AFP, FTP, and SMB. `1`=guests allowed, `0`=guests not allowed. For greater security, do not allow guest access.

For information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Changing SMB Settings for a Share Point

You can use Server Admin to set share point availability through SMB and to change settings such as the share point name that SMB clients see. You can also use Server Admin to set guest access permissions and the default privileges for new files and folders, and to enable opportunistic locking.

For more information about opportunistic locking, see "File Locking with SMB Share Points" on page 94.

To change the settings of an SMB share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point from the list.

4 Click Share Point below the list.

5 Click Protocol Options.

This opens the protocol window with configuration options for AFP, SMB, FTP, and NFS.

6. Click SMB.
7. Provide SMB access to the share point by selecting "Share this item using SMB."
8. Permit unregistered users to have access to the share point by selecting "Allow SMB guest access."

   For greater security, don't select this item.
9. 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.
10. If the share point is only using SMB, select the type of locking for the share point:
    - To permit clients to use opportunistic file locking, select "Enable oplocks."
    - To have clients use standard locks on server files, select "Enable strict locking."
11. If you are using only POSIX permissions, choose a method for assigning default access privileges for new files and folders in the share point:
    - To have new items adopt the privileges of the enclosing item, select "Inherit permissions from parent."
    - To assign specific privileges, select "Assign as follows" and set the Owner, Group, and Everyone privileges using the pop-up menus.
12. Click OK, then click Save.

From the command line:

1. To change SMB settings:

```
$ sudo sharing -e path -s 001 -A customname -g guestflags
```

2. To update the SMB service information to use the new share point settings:

```
$ sudo serveradmin command smb:command = syncPrefs
```

Parameter	Description
path	The full path to the share point.
customname	The name of the share point. If you don't specify the custom name, it's set to the name of the folder, the last name in `path`.
guestflags	A group of flags indicating which protocols allow guest access. The flags are written as a three-digit binary number with the digits representing, from left to right, AFP, FTP, and SMB. `1`=guests allowed, `0`=guests not allowed. For greater security, do not allow guest access.

For information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `sharing` and `serveradmin`, see their man pages. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Changing FTP Settings for a Share Point

You can use Server Admin to set share point availability through FTP and to change settings such as guest access permissions and the share point name that FTP clients see.

To change the settings of an FTP share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Share Point below the list.
5. Click Protocol Options.

   This opens the protocol window with configuration options for AFP, SMB, FTP, and NFS.
6. Click FTP.
7. Make the share point available to FTP clients by selecting "Share this item using FTP."
8. Permit anonymous FTP users to open this item by selecting "Allow FTP guest access."

   For greater security, don't select this item.
9. To change the name clients see when they browse for and connect to the share point using FTP, enter a new name in the "Custom FTP name" field.

   Changing the custom FTP name doesn't affect the name of the share point itself, only the name that FTP clients use.
10. Click OK, then click Save.

From the command line:

- To change FTP settings:

```
$ sudo sharing -e path -s 010 -A customname -g guestflags
```

Parameter	Description
path	The full path to the share point.
customname	The name of the share point. If you don't specify the custom name, it's set to the name of the folder, the last name in `path`.
guestflags	A group of flags indicating which protocols allow guest access. The flags are written as a three-digit binary number with the digits representing, from left to right, AFP, FTP, and SMB. `1`=guests allowed, `0`=guests not allowed. For greater security, do not allow guest access.

For information about command-line parameters for FTP, see "FTP Parameters" on page 146. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Exporting an NFS Share Point

You can use NFS to export share points to UNIX clients. (Export is the NFS term for sharing.)

To export an NFS share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Share Point below the list.
5. Click Protocol Options.

   This opens the protocol window with configuration options for AFP, SMB, FTP, and NFS.
6. Click NFS.
7. Select "Export this item and its contents to" and choose an audience from the pop-up menu.

   To limit clients to specific computers, choose "Client List" and click Add (+) to specify the IP addresses or DNS names of computers that can access the share point.

   To limit clients to the entire subnet, choose "Subnet" and enter the IP address and subnet mask for the subnet.

Important: Make sure the subnet address you enter is the IP network address that corresponds to the subnet mask you chose, and not a client address. Otherwise, your clients can't access the share point.

A network calculator helps you select the subnet address and mask for the range of client addresses you want to serve, and you should use one to validate your final address/mask combination. If needed, network calculators are available on the Web.

For example, suppose you want to export to clients that have IP addresses in the range 192.168.100.50 through 192.168.100.120.

Using a subnet calculator, you discover that the mask 255.255.255.128 applied to any address in this range defines a subnet with a network address of 192.168.100.0 and a range of usable IP addresses from 192.168.100.1 through 192.168.100.126, which includes the desired client addresses.

So, in Server Admin you enter subnet address 192.168.100.0 and subnet mask 255.255.255.128 in the NFS Export Settings for the share point.

To permit unlimited (and unauthenticated) access to the share point, choose "World."

8 From the Mapping pop-up menu, set the privilege mapping for the NFS share point:

- Choose "Root to Root" if you want the root user to have root privileges to read, write, and carry out commands.
- Choose "All to Nobody" if you want users to have minimal privileges to read, write, and carry out commands.
- Choose "Root to Nobody" if you want the root user on a remote client to have only minimal privileges to read, write, and carry out commands.
- Choose "None" if you don't want privileges mapped.

9 From the Minimum Security pop-up menu, set the level of authentication:

- Choose "Standard" if you don't want to set a level of authentication.
- Choose "Any" if you want NFS to accept any method authentication.
- Choose "Kerberos v5" if you want NFS to only accept Kerberos authentication.
- Choose "Kerberos v5 with data integrity" if you want NFS to accept Kerberos authentication and validate the data (checksum) during transmission.
- Choose "Kerberos v5 with data integrity and privacy" to have NFS accept Kerberos authentication, to validate with checksum, and to encrypt data during transmission.

10 If you don't want client users to change the contents of the shared item, select the Read only checkbox.

11 Select Allow subdirectory mounting.

This permits clients to mount subfolders of an exported NFS share point. For example, if you export the /Users/ folder, all its subfolders can be mounted directly.

12 Click OK, then click Save.

Note: If you export more than one NFS share point, you cannot have nested exports on a single volume, which means one exported directory cannot be the child of another exported directory on the same volume.

From the command line:
You can also set up an NFS share point using the command line in Terminal. For information, see the man pages `exports (5)`, `nfs.conf (5)`, and `nfsd (8)`. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Resharing NFS Mounts as AFP Share Points

Resharing NFS mounts (NFS volumes that have been exported to Mac OS X Server) enables Mac OS 9 clients to access NFS file services on traditional UNIX networks.

To reshare an NFS mount as an AFP share point:

1. On the NFS server that's exporting the original share point, make sure the NFS export maps root-to-root so that AFP (which runs as root) can access the files for the clients.
2. Restrict the export to the single AFP server (seen as the client to the NFS server).

   For even greater security, set up a private network for the AFP-to-NFS connection.
3. Open Server Admin and connect to the server.
4. Click File Sharing.
5. Control-click in the Volumes or Share Points list, select Mount NFS Share, then enter the URL of the NFS server you intend to reshare.

   This is the URL that connects to the reshared NFS server. For example, to connect to the reshared NFS mount "widgets" on the root level of the server corp1, usenfs://corp1/widgets.
6. Click OK.

   Server Admin creates the NFS mount point.
7. Follow steps 1 through 6 for each NFS volume you want to reshare.
8. Using Server Admin, share the NFS mounts as AFP share points.

   The NFS mounts appear as normal volumes in the Share Point list. (You can also share the NFS mounts using SMB and FTP, but you should use only AFP.)

   You can change privileges and ownership, but you can't enable quotas (because quotas work only on local volumes). However, if quotas are enabled on the NFS server, they apply to the reshared volume.

   Note: Quotas set on the original NFS export are enforced on the AFP reshare.

Automatically Mounting Share Points for Clients

You can mount share points automatically on client Mac OS X computers using network mounts. You can automatically mount AFP or NFS share points.

When you set a share point to automatically mount, a mount record is created in the Open Directory domain. Be sure you create these records in the same shared domain where the user and computer records exist.

Note: All users have guest access to network automounted AFP share points. Authenticated access is permitted only for a user's own home folder or if you have Kerberos set to support single sign-on (SSO) authentication.

To set up a network mount:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point from the list.
4. Click Share Point below the list.
5. Select the Enable Automount checkbox.

   This opens a configuration window for the automount.
6. From the Directory pop-up menu, choose the directory domain that contains your users and computers.
7. From the Protocol pop-up menu, choose the sharing protocol (AFP or NFS).

   If you choose AFP, guest access must be enabled for automounted AFP share points to work, except when all users have access to their home folders using Kerberos SSO authentication. For more information, see "Configuring AFP Service Access Settings" on page 71.
8. Choose how you want the share point to be used and mounted on client computers:
   - **User home folders and group folders:** Select to have the home folders and group folders on the share point listed on a user's computer in /Network/Servers/.
   - **Shared Applications folder:** Select to have the share point appear in /Network/Applications/ on the user's computer.
   - **Shared Library folder:** Select to have the share point appear in /Network/Library/. This creates a network library.
   - **Custom mount path:** Select to have the share point appear in the folder you specify. Before you mount the share point, be sure this folder exists on the client computer.
9. Click OK.
10. Authenticate when prompted.
11. Click Save.

Mounting a user's home folder

To mount a user's home folder, use `mnthome`. The `mnthome` tool unmounts the AFP home folder that was automounted as guest, and remounts it with the correct privileges by logging into the AFP server using the current user name and password.

- To mount a user's shared home folder on an AFP server:

```
$ mnthome -p password
```

For more information, see the `mnthome` man page.

Managing Share Points

This section describes day-to-day tasks you might perform after you set up share points on your server. Initial setup information appears in "Setting Up a Share Point" on page 36.

Checking File Sharing Status

Use Server Admin to check the status of volumes and share points.

To view File Sharing status:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Volumes to see a list of volumes.
4. Click List to view the volumes details.

   Each volume includes the disk space used and the type of volume.
5. Click Share Points to see a list of share points and their pathnames.
6. Click List to see share point details.

   Each share point includes the disk space used and whether sharing, guest access, automount, Spotlight indexing, and Time Machine are enabled or disabled.
7. To monitor the quotas setup for a volume, select the volume and click Quotas below the volume list.

Disabling a Share Point

To stop sharing a share point, use File Sharing in Server Admin to remove it from the Share Points list.

Note: Before you delete or rename a share point in Finder, disable the share point in Server Admin.

To remove a share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.

3 Click Share Points and select the share point you want to remove.

4 Click Unshare.

5 Click Save.

Protocol and network mount settings you made for the item are discarded.

From the command line:

- To delete a share point:

```
$ sudo sharing -r path
```

Parameter	Description
path	The full path to the share point.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Disabling a Protocol for a Share Point

You can use File Sharing in Server Admin to stop sharing a share point using a specific protocol and still permit sharing to continue through other protocols.

To stop sharing through a specific protocol:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to reconfigure.

4 Click Share Point below the list.

5 Click Protocol Options and select the protocol.

6 For AFP, SMB, and FTP, deselect the "Share this item using" checkbox; for NFS, deselect the "export this item and its contents to" checkbox.

You can disable a protocol for all share points by stopping the underlying service that provides support for the protocol. For more information, see "Stopping AFP Service" on page 79, "Stopping NFS Service" on page 113, or "Stopping FTP Service" on page 134.

From the command line:

- To disable protocol sharing for a share point:

```
$ sudo sharing -e path -s shareflags
```

Parameter	Description
path	The full path to the share point.
shareflags	A three-digit binary number indicating the protocols used to share the folder. The digits represent, from left to right, AFP, FTP, and SMB. `1`=shared, `0`=not shared.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing Share Point Configuration and Protocol Settings

You can view share point configuration and protocol settings in Server Admin from the Share Points list.

To view the share point configuration and protocol settings on a server:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points.
4. Click List to view the share point details.

   You can view the share point name, path, disk space, sharing, guest access, automount, Spotlight, and Time Machine settings.

   Use tooltips to quickly display the shared and guest access protocols for a share point.
5. Select the share point and click Share Point below the list.
6. View the protocol settings by clicking Protocol Options and selecting the protocol (AFP, SMB, FTP, or NFS).

From the command line:

- To view share point settings:

  ```
  $ sudo sharing -l
  ```

  For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing Share Point Content and Privileges

You can use File Sharing in Server Admin to view share point content and access privileges.

To view share point content and access privileges on a server:

1. Open Server Admin and connect to the server.
2. Click File Sharing.

3 Click Share Points and select a share point in the list.

4 Click Browse.

5 Click Permissions below the list.

You can now view the contents of the selected share point and access items in the folder hierarchy. You can also view the privilege settings (POSIX and ACL) of the share point and each item in the folder hierarchy.

From the command line:

- To view share points:

```
$ sudo sharing -l
```

- To view share point content:

```
$ ls path
```

Parameter	Description
path	The full path to the share point.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing` and `ls`, see their man pages. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Managing Share Point Access Privileges

This section describes typical tasks you perform to manage access privileges for a share point.

Changing POSIX Permissions

You use Server Admin to view and change standard POSIX permissions for a share point.

To change standard POSIX permissions for a share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to update from the list.

4 Click Permissions below the list.

To alter the POSIX permissions, change the owner and group of the shared item by dragging names from the Users & Groups window to the User/Group field in the permissions table or by entering a user or group name in the User/Group field.

The owner and group records are listed under the POSIX heading. The owner record is the one with the single user icon and the group record is the one with the group icon.

Open the Users & Groups window by clicking Add (+).

5 To change the permissions for the Owner, Group, and Others (Everyone), use the Permissions pop-up menu in the related row of the permissions table.

Others is any user who is not the owner and does not belong to the group but can log in to the file server.

From the command line:

- To change permissions for an item:

```
$ chmod securitygroupchangetypepermissionfileorfolder
```

Parameter	Description
securitygroup	The person or group whose permission you are changing: • u—user • g—group • o—other • all—all
changetype	The type of change you are making. To add or subtract permission: • "+"—add permission • "-"—remove permission
permission	The permission you are changing: • r—read • w—write • e—execute
fileorfolder	The name of the file or folder to change.

For information about `chmod`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Adding ACEs to ACLs

You control access to a share point by adding or removing ACEs to the share point ACL. Each ACE defines the access permissions for a user or a group.

To add an ACE to an ACL:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to update from the list.

4 Click Permissions below the list.

5 Open the Users & Groups window by clicking Add (+).

6 Drag users and groups you want to add to the access control list.

7 Click Save.

By default, each new ACE gives the user or group full read permissions. In addition, all four inheritance options are selected. For more information about inheritance options, see "To see the most recent server help topics:" on page 10. To change ACE settings, see "Editing ACEs" on page 52.

From the command line:

- To add an ACE:

```
$ sudo chmod +a file1
```

Parameter	Description
file1	The name of the file you are adding.

For information about about `chmod`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Removing ACEs

You control access to a share point by adding or removing ACEs to the share point ACL. Each ACE defines the access permissions for a user or a group.

To delete an ACE from an ACL:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Permissions below the list.
5. In the Access Control List, select the ACE.
6. Click Delete (–).
7. Click Save.

From the command line:

- To delete an ACE:

```
$ sudo chmod -a file1
```

Parameter	Description
file1	The name of the file you are deleting.

For information about `chmod`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Editing ACEs

Use Server Admin to change the settings of an ACE to permit or restrict a user or group from performing specific tasks in a share point.

To edit an ACE:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Permissions below the list.
5. In the Access Control List, select the ACE.
6. Click the Edit (/) button.
7. From the Permission Type pop-up menu, choose "Allow" or "Deny."
8. In the Permission list, select permissions.
9. Click OK.
10. Click Save.

You can also edit an ACE's Type and Permission fields by clicking the field and choosing an option from the pop-up menu. The Permission field provides five options:

- Full Control
- Read and Write
- Read
- Write
- Custom (which displays if the permissions set don't match any other options)

For more information about permissions and permission types, see "Access Control Entries (ACEs)" on page 23.

Sorting an ACL Canonically

In Server Admin, an ACL can be sorted by Type. When sorting canonically, Server Admin first lists all entries with a Type of Deny, then the entries with the Allow Type.

To sort an ACL canonically:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Permissions below the list.
5. From the Action menu button (gear), choose "Sort Access Control List Canonically."
6. Click Save.

Removing a Folder's Inherited ACEs

If you don't want to apply inherited ACEs to a folder or a file, you can remove these entries using Server Admin.

Inherited ACEs appear dimmed unless you chose to make them explicit, as described in "Changing Inherited ACEs for a Folder to Explicit" on page 54.

To remove a folder's inherited ACEs:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Browse and select the folder.
5. Click Permissions below the list.
6. From the Action menu button (gear), choose "Remove Inherited Entries."
7. Click Save.

   Server Admin removes the inherited ACEs.

From the command line:

- To remove an inherited ACE:

```
$ sudo chmod -ai file1
```

Parameter	Description
file1	The name of the file you are removing.

For information about `chmod`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Changing Inherited ACEs for a Folder to Explicit

Inherited ACEs appear dimmed in the ACL of Server Admin and you can't edit them. To change ACEs for a folder, change the inheritance to explicit.

To change inherited ACEs of a folder to explicit:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Browse and select the folder.
5. Click Permissions below the list.
6. From the Action menu button (gear), choose "Make Inherited Entries Explicit."
7. Click Save.

   You can now edit the ACEs.

Propagating Permissions

Server Admin enables you to specify which permissions to propagate to descendant files and folders. In the case of POSIX permissions, you can specify the following to propagate:

- Owner name
- Group name
- Owner permissions
- Group permissions
- Others permissions

The ability to select which information to propagate gives you specific control over who can access files and folders.

For ACL permissions, you can only propagate the entire ACL. You can't propagate individual ACEs.

To propagate folder permissions:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. If you want to propagate permissions for a specific folder, click Browse and select the folder.
5. Click Permissions below the list.
6. From the Action menu button (gear), choose "Propagate Permissions."
7. Select the permissions you want to propagate.
8. Click OK.

Server Admin propagates the selected permissions to all descendants.

Removing an ACL from a File or Folder

To remove an inherited ACL from a file or folder, use Server Admin.

Note: Because the ACEs of a file are usually inherited, they might appear dimmed.

To remove an ACL from a file or folder:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Permissions below the list.
5. Click Browse and select the file or folder.
6. Select all ACEs in the ACL Permissions list and click Delete (–).

7 Click Save.

Server Admin removes all ACEs from the ACL of a file. The only permissions that now apply are standard POSIX permissions.

From the command line:

- To remove a file's ACL:

```
$ chmod -a file1
```

Parameter	Description
file1	The name of the file whose ACL you are removing.

For information about `chmod`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Applying ACL Inheritance to a File or Folder

If you removed the ACL from a file or folder and want to restore it, use Server Admin.

To apply ACL inheritance to a file or folder:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to update from the list.

4 Click Browse and select the file or folder.

5 Click Permissions below the list.

6 From the Action menu button (gear), choose "Propagate Permissions."

7 Select Access Control List.

8 Click OK, then click Save.

Determining a User's File or Folder Permissions

To instantly determine the permissions that a user has to a file or folder, use the Effective Permission Inspector in Server Admin.

To determine a user's file or folder permissions:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to update from the list.

4 Click Permissions below the list.

5 From the Action menu button (gear), choose "Show Effective Permission Inspector."

Permissions and inheritance settings are dimmed to indicate that you can't edit them.

6 Open the Users & Groups window by clicking the Add (+) button (below the Permissions list).

7 From the Users & Groups window, drag a user to the Effective Permission Inspector.

If you don't see a recently created user, click the Refresh button (below the Servers list).

After dragging the user from the list, the inspector shows the permissions the user has for the selected file or folder. An entry with a checkmark means the user has the indicated permission (equivalent to Allow). An entry without a checkmark means the opposite (equivalent to Deny).

8 When you finish, close the inspector window.

Changing the Protocols Used by a Share Point

You can use Server Admin to change the protocols available for accessing a share point. The following protocols are available:

- AFP (see "Changing AFP Settings for a Share Point" on page 39)
- SMB (see "Changing SMB Settings for a Share Point" on page 40)
- FTP (see "Changing FTP Settings for a Share Point" on page 42)
- NFS (see "Exporting an NFS Share Point" on page 43)

To change the protocols for a share point:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to update from the list.

4 Click Share Point below the list.

5 Click Protocol Options and select the protocol.

6 Select the protocols you want to change and modify the configuration.

7 Click OK, then click Save.

From the command line:

- To change the protocol settings of a share point:

```
$ sudo sharing -e path -s shareflags
```

Parameter	Description
path	The full path to the share point.
shareflags	A three-digit binary number indicating the protocols used to share the folder. The digits represent, from left to right, AFP, FTP, and SMB. `1`=shared, `0`=not shared.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

You can't configure NFS protocols using the `sharing` command. For more about changing NFS protocols, see the man pages `exports (5)`, `nfs.conf (5)`, and `nfsd (8)`.

Changing NFS Share Point Client Access

You can use Server Admin to restrict the clients that can access an NFS export.

To change authorized NFS clients:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the NFS share point.
4. Click Protocol Options and select NFS.
5. Select the "Export this item and its contents to" checkbox and choose an option from the pop-up menu:
   - To limit clients to specific computers, choose Client List, click Add (+), and then enter the IP addresses or DNS names of computers that can access the share point.
   - To remove a client, select an address from the Client List and click Delete (–).
   - To limit clients to the entire subnet, choose Subnet and enter the IP address and subnet mask for the subnet.
   - To permit unlimited (and unauthenticated) access to the share point, choose World.
6. Click OK, then click Save.

Enabling Guest Access to a Share Point

You can use Server Admin to enable guest users (users not defined in the directories used by your server) to connect to specific share points.

Note: This section does not apply to NFS.

To change guest access privileges for a share point:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to update from the list.
4. Click Share Point below the list.
5. Click Protocol Options and select the protocol you are using to provide access to the share point.
6. Select the "Allow guest access" option.

7 Click OK, then click Save.

Note: Make sure guest access is also enabled at the service level in Server Admin.

From the command line:

- To enable guest access to a share point:

```
$ sudo sharing -a path -g 1
```

Parameter	Description
path	The full path to the share point.

For information about command-line parameters, see "Creating a Share Point" on page 140. For information about `sharing`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Setting Up a Drop Box

A drop box is a shared folder with custom permissions. If you use only ACLs, you can set permissions so that specific users can only copy files to the folder but can't see its contents. If you use only POSIX permissions, you can set them to permit anyone to copy files to the drop box but give only the owner of the drop box full access.

To create a drop box:

1 Create the folder that will act as a drop box in an AFP share point.

2 Open Server Admin and connect to the server.

3 Click File Sharing.

4 Click Share Points.

5 Click Browse and select the folder in the AFP share point that you want to use as a drop box.

6 Click Permissions below the list.

7 Set write only permissions using POSIX permissions or a combination of POSIX permissions and ACEs.

To create a drop box using standard permissions, set Write Only permissions for Owner, Group, and Others. For more information, see "Setting Standard Permissions" on page 37.

Note: For greater security, assign None to Others.

To create a drop box using ACL permissions, add two types of ACEs:

- If you want users to only copy items to a drop box but not see its contents, add ACEs that deny them Administration and Read permissions and give only Traverse Folder, Create File (Write Data), and Create Folder (Append Data) permissions.
- If you want users to have full control of the drop box, add ACEs that give them full Administration, Read, Write, and inheritable permissions.

For more information, see "Setting ACL Permissions" on page 38.

8 Click Save.

From the command line:

1 Create the folder that will act as a drop box in an AFP share point:

```
$ sudo mkdir path/folder1
```

2 Add permissions for the folder:

```
$ chmod securitygroup + permissionfolder1
```

Parameter	Description
path	The full path to the share point.
folder1	The folder that will be the drop box.
securitygroup	The person or group whose permission you are changing. Can be the following: • u—user • g—group • o—other • all—all
permission	The permission you are changing: • r—read • w—write • e—execute

For information about `mkdir` and `chmod`, see their man pages. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Setting Up a Network Library

Configuring a network library creates a repository on the network for shared information such as default configurations, fonts, images, and other common resources.

A shared library is automatically mounted at /Network/Library/ and is accessible through Finder. Guest access must be enabled to grant all users access to the network library. All users or groups who are logged into the network with guest access have access to this shared information, and the network library becomes part of the default search path. Access to the network library can be restricted using access controls.

To configure a network library:

1 Open Server Admin and connect to the server.

2 Click File Sharing.

3 Click Share Points and select the share point you want to become a network library.

To create a share point for your network library, see "Creating a Share Point" on page 36.

4. Click Share Point below the list.
5. Select the Enable Automount checkbox.
6. From the Directory pop-up menu, choose the directory domain that contains your users and computers.
7. From the Protocol pop-up menu, choose the sharing protocol (AFP or NFS).

   If you choose AFP, guest access must be enabled for automounted AFP share points to work, except when all users have access to their home folders using Kerberos SSO authentication. For more information, see "Configuring AFP Service Access Settings" on page 71.
8. Choose "Shared Library folder" for the share point to appear in /Network/Library/.
9. Click OK.
10. Authenticate when prompted.
11. Click Save.

Using Mac OS X Server for Network Attached Storage

You can configure Mac OS X Server for Network Attached Storage (NAS), to provide basic NAS-style file resharing using AFP, SMB, FTP, and NFS as well as advanced features such as directory integration. NAS also works with more advanced storage architectures such as RAID data protection and Xsan for storage clustering.

To provide NAS-style file sharing for network users, you must configure your Mac OS X server for NAS. The most common configuration uses an Xserve unit (as a file server) with a RAID device (data storage). You can also use Xsan for a more advanced NAS configuration.

The steps that follow explain how to set up an Xserve NAS system.

Step 1: Connect the Xserve system to the network The Xserve system has gigabit Ethernet hardware for extremely fast communications with other network devices. Data transmission rates are determined by the speed of other components, such as the network hub or switch and cables used.

If you are also using a RAID unit as part of the NAS system, connect it to the Xserve unit by installing the Apple Fibre Channel PCI card in the Xserve unit and installing the Fibre Channel cables between the two hardware components.

To assure that connecting the system to the network does not disrupt network operations, work with the system administrator or other expert. Follow the instructions in the Xserve guide, if applicable, to install the system properly in a rack.

Step 2: Establish volumes, partitions, and RAID sets on the drive modules Plan how you want to divide the total storage on the Xserve NAS system, taking into account the number of users, likely demands for NAS, and future growth.

Then use Disk Utility to create partitions or RAID arrays on the drives. If you have a RAID, use RAID Admin to create RAID arrays on the drives and Disk Utility to put the file system on the arrays.

For information about using these applications, consult the Disk Utility online help and the RAID Admin documentation.

You can also use Xsan to configure partitions and RAID configurations. For more information about Xsan, see the Xsan documentation.

Step 3: Set up the system as a network-attached storage device If you purchased a new Xserve unit, Mac OS X Server software is already installed. You only need to perform initial server setup by turning on the system and answering the questions posed by Server Assistant. Make sure you enter a fixed IP address for the server, either static or using DHCP with a manual address.

If you need to install Mac OS X Server software, use *Getting Started* to understand system requirements and installation options posed by Server Assistant.

Note: You can set up Xserve NAS remotely or locally. If you are setting up from a remote computer, install the applications on the Admin Tools disc on the remote computer. If you are configuring locally, connect a monitor and keyboard to your Xserve unit. The system must have a video card for direct connection of a monitor. A video card is optional on some Xserve models, including the Xserve G5.

To perform initial setup for NAS:

1. Make sure the system is connected to the network.
2. Open Server Admin and enable the AFP, NFS, FTP, and SMB services so they are available for use immediately.

   If you want users to share files using FTP, be sure your network is securely configured.

   AFP is the standard for Mac OS X files. NFS is the file protocol for UNIX and Linux users. SMB includes Server Message Block (SMB) protocol, which supports Microsoft Windows 95, 98, ME (millennium Edition), NT 4.0, 2000, XP, and Vista. FTP allows access to shared files by anyone who connects to the NAS system.

Step 4: Configure file services for AFP, NFS, FTP, and SMB Assuming that you turned on the file services with Server Admin, you can configure AFP, NFS, FTP, and SMB so that clients on the network can share their files. The summary instructions that follow provide an overview of configuring these file services.

For more information about configuring these protocols, see the related chapter in this guide.

Step 5: Set up share points and access privileges for the Xserve NAS Use Server Admin to set share points and define access privileges for share points. For more information, see "Setting Up a Share Point" on page 36.

After you finish these steps, the basic setup of the Xserve NAS system is complete. You can add or change share points, users, and groups when necessary.

Configuring Spotlight for Share Points

If your client computers need to search share points, you can enable Spotlight indexing in Server Admin.

Spotlight indexing is only available for a share point that has AFP or SMB turned on. If your share point does not use AFP or SMB, do not enable Spotlight searching.

If you have a share point with Spotlight turned on and you turn off AFP and SMB, Spotlight indexing will not work.

If you are using an Xsan volume and want to enable or disable Spotlight, use Xsan Admin.

Spotlight provides the capability to do quick searches of network volumes, which requires the server to maintain an index of all files and folders on a share point. This indexing process uses more server resources. To free these resources, turn off Spotlight if not used.

To configure Spotlight for share points:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to enable Spotlight for.
4. Click Share Point below the list.
5. Select the Enable Spotlight searching checkbox.
6. Click Save.

From the command line:

- To enable Spotlight for a volume:

```
$ sudo mdutil -i on volume
```

- To disable Spotlight for a volume:

```
$ sudo mdutil -i off volume
```

Configuring Time Machine Backup Destination

Time Machine is a backup application that keeps an up-to-date copy of everything on your computer, which includes system files, applications, accounts, preferences, and documents. Time Machine can restore files, folders, or your entire computer by putting everything back the way it was and where it should be.

Selecting this option causes the share to be broadcast over Bonjour as a possible Time Machine destination, so it shows up as an option in System Preferences. On a standard or workgroup server, selecting this option also sets POSIX permissions to 770 and the POSIX group to com.apple.access_backup.

You can designate a share point as a Time Machine backup in Server Admin.

To configure a Time Machine backup destination:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Share Points and select the share point you want to become the Time Machine backup destination.
4. Click Share Point below the list.
5. Select the "Enable as Time Machine backup destination" checkbox.
6. Click Save.

Configuring Share Point Quotas

You can set the maximum size of a user's home folder by setting a quota on the Home pane of the user's account settings in Workgroup Manager.

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 domain 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.

From the command line:

- To set disk quotas for users on a share point:

```
$ sudo edquota -u -p proto-username username ...
```

- To set disk quotas for groups on a share point:

```
$ sudo edquota -u -p proto-groupname groupname ...
```

- To set the grace period for enforcing disk quotas for users:

```
$ sudo edquota -t -u
```

- To set the grace period for enforcing disk quotas for groups:

```
$ sudo edquota -t -g
```

Note: You can specify the default grace period in /usr/include/sys/quota.h. For a user, you specify the grace period in the file .quota.ops.user located at the root of the user's mounted file system. For a group, you specify the grace period in the file .quota.ops.group located at the root of the group's mounted file system.

Parameter	Description
proto-username	The user whose disk quota will be duplicated to other users.
username	The user whose disk quota should be set to the same quota as *proto-username*. `1`=shared, `0`=not shared.
proto-groupname	The group whose disk quota will be applied to other groups.
groupname	The group whose disk quota should be set to the same quota as *proto-groupname*.

For information about `edquota`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Monitoring Share Point Quotas

Use Server Admin to view the space on a volume allocated for a user. This space (disk quota), configured in Workgroup Manager, is the maximum size of a user's home folder.

To monitor share point quotas:

1. Open Server Admin and connect to the server.
2. Click File Sharing.
3. Click Volumes and select the volume you want to monitor.
4. Click Quotas below the list.
5. Select the "Enable quotas on this volume" checkbox.

The disk quota information for the enabled volumes is listed in the Quota Monitor. This includes user name, space used (KB), free space (KB), and limit (KB).

6 Click Save.

Setting SACL Permissions

SACLs enable you to specify who has access to AFP, FTP, and SMB file services. This provides you with greater control over who can use the services and which administrators have access to monitor and manage the services.

Setting File Services SACL Permissions for Users and Groups

Use Server Admin to set SACL permissions for users and groups to access file services.

To set user and group SACL permissions for a file service:

1 Open Server Admin and connect to the server.

2 Click Settings.

3 Click Access.

4 Click Services.

5 Select the level of restriction you want for services:

- To restrict access to all services, select "For all services."
- To set access permissions for individual services, select "For selected services below" and then select the services from the service list.

6 Select the level of restriction you want for users and groups:

- To provide unrestricted access, click "Allow all users and groups."
- To restrict access to specific users and groups, select "Allow only users and groups below," click Add (+) to open the Users & Groups window, and then drag users and groups from the Users & Groups window to the list.

7 Click Save.

Setting Files Services SACL Permissions for Administrators

Use Server Admin to set SACL permissions for administrators to monitor and manage file services.

To set administrator SACL permissions for a file service:

1 Open Server Admin and connect to the server.

2 Click Settings.

3 Click Access.

4 Click Administrators.

5 Select the level of restriction that you want for the services:

- To restrict access to all services, select "For all services."
- To set access permissions for individual services, select "For selected services below" and then select services from the service list.

6 Click Add (+) to open the Users & Groups window.

7 Drag users and groups to the list.

8 Set the user's permission:

- To grant administrator access, choose Administer from the Permission pop-up menu next to the user name.
- To grant monitoring access, choose Monitor from the Permission pop-up menu next to the user name.

9 Click Save.

Working with AFP Service

4

Use this chapter to set up and manage AFP Service in Mac OS X Server.

Apple Filing Protocol (AFP) service enables Mac OS clients to connect to your server and access folders and files. Non-Mac OS clients can also connect to your server over AFP using third-party AFP client software.

AFP service supports new features such as Unicode file names, access control lists (ACLs), 64-bit file sizes, extended attributes, and Spotlight searching. Unicode is a standard that assigns a unique number to every character regardless of the language or the operating system used to display the language.

Kerberos Authentication

AFP supports Kerberos authentication. Kerberos is a network authentication protocol developed at MIT to provide secure authentication and communication over open networks.

In addition to the standard authentication method, Mac OS X Server uses Generic Security Services Application Programming Interface (GSSAPI) authentication protocol. GSSAPI is used to authenticate using Kerberos v.5. You specify the authentication method using the Access pane of the AFP service settings in Server Admin.

For information about setting up AFP, see "Configuring AFP Service Access Settings" on page 71. For information about setting up Kerberos, see *Open Directory Administration*.

AppleTalk Support

AFP service no longer supports AppleTalk as a client connection method. Although AppleTalk clients can see AFP servers in the Chooser, they must use TCP/IP to connect to these servers.

For more information, see "Mac OS X Clients" on page 89 and "Connecting to the AFP Server from Mac OS 8 and Mac OS 9 Clients" on page 92.

AFP Service Specifications

AFP service has the following default specifications:

- Maximum number of connected users, depending on your license agreement: Unlimited (hardware dependent)
- Maximum volume size: 16 terabytes
- TCP port number: 548
- Location of log files: /Library/Logs/AppleFileService/
- Bonjour registration type: afpserver

Setup Overview

Here is an overview of the basic steps for setting up AFP service.

Step 1: Turn AFP service on Before configuring AFP service, AFP must be turned on. See "Turning AFP Service On" on page 69.

Step 2: Configure AFP General settings Configure the General settings to advertise the AFP share point, enable Mac OS 8 and Mac OS 9 clients to find the server, and specify a login greeting. See "Configuring AFP Service General Settings" on page 70.

Step 3: Configure AFP Access settings Use Access settings to permit guest AFP users, limit the number of simultaneous Windows client connections, or set AFP authentication options. See "Configuring AFP Service Access Settings" on page 71.

Step 4: Configure AFP Logging settings Use Logging settings to specify how much information is recorded in AFP log files. See "Configuring AFP Service Logging Settings" on page 73.

Step 5: Configure AFP Idle Users settings Use Idle Users settings to disconnect idle clients, enable clients to reconnect after sleeping (within a specified time limit), and customize a disconnect message. See "Configuring AFP Service Idle Users Settings" on page 74.

Step 6: Start AFP service After you configure AFP, start the service to make it available. See "Starting AFP Service" on page 76.

Turning AFP Service On

Before you can configure AFP settings, you must turn on AFP service in Server Admin.

To turn AFP service on:

1. Open Server Admin and connect to the server.
2. Click Settings, then click services.
3. Select the AFP checkbox.
4. Click Save.

Setting Up AFP Service

If you enabled the Server Assistant to start AFP service when you installed Mac OS X Server, you don't need to do anything else. Verify that the default service settings meet your needs.

There are four groups of settings on the Settings pane for AFP service in Server Admin:

- **General.** Sets information that identifies your server, enables automatic startup, and creates a login message for AFP service.
- **Access.** Sets up client connections and guest access.
- **Logging.** Configures and manages logs for AFP service.
- **Idle Users.** Configures and administers idle user settings.

The following sections describe how to configure these settings and how to start AFP service when you finish.

Configuring AFP Service General Settings

Use the General settings pane in AFP service to enable automatic startup, enable browsing with Bonjour, and create a login greeting for your users.

To configure AFP service General settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click General.
5. If you have Mac OS 8 and Mac OS 9 clients with special language needs, choose the correct character set from the "Encoding for older clients" pop-up menu.

   When Mac OS 9 (or earlier) clients are connected, the server converts file names from the system's UTF-8 character encoding to the chosen set. This has no effect on Mac OS X client users.
6. Enter the message you want users to see in the Login Greeting field.

   The message does not appear when a user logs in to their home folder.

   To prevent users from seeing the greeting repeatedly, select "Do not send same greeting twice to the same user."
7. Click Save.

From the command line:

- To change several settings:

```
$ sudo serveradmin settings
afp:registerNSL = value
```

```
afp:afpServerEncoding = value
afp:loginGreeting = "value"
Control-D
```

- To view all AFP service settings:

```
$ sudo serveradmin settings afp
```

Parameter	Description
`registerNSL`	Advertise the server using Bonjour. Default = `yes`
`afpServerEncoding`	Encoding used with Mac OS 9 clients. Default = `0`
`loginGreeting`	Login greeting message. Default = `""`

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring AFP Service Access Settings

Use the Access pane of AFP service in Server Admin to control client connections and guest access.

To configure AFP service Access settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Access.
5. Choose the authentication method you want to use from the Authentication pop-up menu: Standard, Kerberos, or Any Method.
6. If necessary, permit unregistered users to access AFP share points by selecting "Enable Guest access."

   Guest access is a convenient way to provide occasional users with access to files and other items, but for better security, don't select this option.

   Note: After you permit guest access for AFP service in general, you can still selectively enable or disable guest access for individual share points.
7. Enable an administrator to log in using a user's name with an administrator password (and thereby experience AFP service as the user would) by selecting "Enable administrator to masquerade as any registered user."

8 Restrict the number of simultaneous client connections by clicking the button next to the Client Connections or Guest Connections field, then enter a number.

The maximum number of simultaneous users is limited by the type of license you have. For example, if you have a 10-user license for your server, a maximum of 10 users can connect at one time.

Select Unlimited if you do not want to restrict the maximum number of connections. The maximum number of guests cannot exceed the maximum number of total client connections permitted.

9 Click Save.

From the command line:

- To change several settings:

```
$ sudo serveradmin settings
afp:authenticationMode = "value"
afp:guestAccess = value
afp:attemptAdminAuth = value
afp:maxConnections = value
afp:maxGuests = value
Control-D
```

- To view all AFP service settings:

```
$ sudo serveradmin settings afp
```

Parameter	Description

`authenticationMode`	Authentication mode. Can be:
	`standard`
	`kerberos`
	`standard_and_kerberos`
	Default = `"standard_and_kerberos"`

`guestAccess`	Allow guest users access to the server. Default = `yes`
`attemptAdminAuth`	Allow administrator user to masquerade as another user. Default = `yes`
`maxConnections`	Maximum simultaneous user sessions allowed by the server. Default = `-1` (unlimited)
`maxGuests`	Maximum simultaneous guest users allowed. Default = `-1` (unlimited)

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring AFP Service Logging Settings

Use the Logging pane of AFP service in Server Admin to configure and manage service logs.

To configure AFP service Logging settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Logging.
5. To keep a record of users who connect to the server using AFP, select "Enable access log."
6. To periodically close and save the active log and open a new one, select "Archive every __ days" and enter the number of days after which the log is archived.

   The default is 7 days. The server closes the active log at the end of each archive period, renames it to include the current date, and then opens a new log file.
7. Select the events you want AFP service to log.

   An entry is added to the log when a user performs an action you select.

   When you choose the number of events to log, consider available disk space. The more events you choose, the faster the log file will grow.
8. To specify how often the error log file contents are saved to an archive, select "Error Log: Archive every __ days" and enter the number of days.
9. Click Save.

   You can keep the archived logs for your records or manually delete them to free disk space when they're no longer needed. Log files are stored in /Library/Logs/AppleFileService/. You can use the log rolling scripts supplied with Mac OS X Server to reclaim disk space used by log files.

From the command line:

- To change AFP service Logging settings:

```
$ sudo serveradmin settings
afp:activityLog = value
afp:activityLogTime = value
afp:loggingAttributes:logLogin = value
afp:loggingAttributes:logLogout = value
```

```
afp:loggingAttributes:logOpenFork = value
afp:loggingAttributes:logCreateFile = value
afp:loggingAttributes:logCreateDir = value
afp:loggingAttributes:logDelete = value
afp:errorLogTime = value
Control-D
```

- To view all AFP service settings:

```
$ sudo serveradmin settings afp
```

Parameter	Description
`activityLog`	Turn activity logging on or off. Default = `no`
`loggingAttributes: logLogin`	Record user logins in the activity log. Default = `yes`
`loggingAttributes: logLogout`	Log user logouts in the activity log. Default = `yes`
`loggingAttributes: logOpenFork`	Log file opens in the activity log. Default = `yes`
`loggingAttributes: logCreateFile`	Record file creations in the activity log. Default = `yes`
`loggingAttributes: logCreateDir`	Record folder creations in the activity log. Default = `yes`
`loggingAttributes: logDelete`	Record file deletions in the activity log. Default = `yes`
`activityLogTime`	Rollover time (in days) for the activity log. Default = `7`

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring AFP Service Idle Users Settings

Use the Idle Users pane of AFP service to specify how your server handles idle users. An idle user is someone who is connected to the server but whose connection has been inactive for a predefined period of time.

If a client is idle or asleep for longer than the specified idle time, open files are closed, the client is disconnected, and unsaved work is lost.

To configure Idle Users settings:

1. Open Server Admin and connect to the server.

2. Click the triangle at the left of the server.

   The list of services appears.

3. From the expanded Servers list, select AFP.

4. Click Settings, then click Idle Users.

5. To enable client computers to reconnect after sleeping for a specific time, select "Allow clients to sleep __ hours" and enter a number in the related field.

   Sleeping clients will not show as idle.

   Although the server disconnects sleeping clients, the clients' sessions are maintained for the specified period. A sleeping Mac OS X v10.2 (or later) client can resume work on open files within the limits of the "Allow clients to sleep" setting.

6. To specify the idle time limit, select "Disconnect idle users after __ minutes" and enter the number of minutes after which the AFP session of an idle connection is disconnected.

   To prevent specific types of users from being disconnected, select them under "Except."

7. In the "Disconnect Message" field, enter the message you want users to see when they are disconnected.

   If you don't enter a message, a default message appears stating that the user has been disconnected because the connection has been idle for a period of time.

8. Click Save.

From the command line:

- To change AFP service Idle User settings:

```
$ sudo serveradmin settings
afp:clientSleepOnOff = value
afp:clientSleepTime = value
afp:idleDisconnectOnOff = value
afp:idleDisconnectTime = value
afp:idleDisconnectFlag:guestUsers = value
afp:idleDisconnectFlag:adminUsers = value
afp:idleDisconnectFlag:registeredUsers = value
afp:idleDisconnectFlag:usersWithOpenFiles = value
afp:idleDisconnectMsg = "value"
Control-D
```

- To view all AFP service settings:

```
$ sudo serveradmin settings afp
```

Parameter	Description
`clientSleepOnOff`	Allow client computers to sleep. Default = `yes`
`clientSleepTime`	Time (in hours) that clients are allowed to sleep. Default = `24`
`idleDisconnectOnOff`	Enable idle disconnect. Default = `no`
`idleDisconnectTime`	Idle time (in minutes) allowed before disconnect. Default = `10`
`idleDisconnectFlag: guestUsers`	Enforce idle disconnect for guest users. Default = `yes`
`idleDisconnectFlag: adminUsers`	Enforce idle disconnect for administrator users. Default = `yes`
`idleDisconnectFlag: registeredUsers`	Enforce idle disconnect for registered users. Default = `yes`
`idleDisconnectFlag: usersWithOpenFiles`	Enforce idle disconnect for users with open files. Default = `yes`
`idleDisconnectMsg`	Idle disconnect message. Default = `""`

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Starting AFP Service

You start AFP service to make AFP share points available to your client users.

To start AFP service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Start AFP (below the Servers list).

   The service runs until you stop it and restarts if your server is restarted.

From the command line:

- To start AFP service:

```
$ sudo serveradmin start afp
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Managing AFP Service

This section describes typical day-to-day tasks you perform after you set up AFP service on your server. Initial setup information appears in "Setting Up AFP Service" on page 70.

Checking AFP Service Status

Use Server Admin to check the status of AFP service.

To view AFP service status:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. To see information such as whether the service is running, when it started, its throughput, the number of connections, and whether guest access is enabled, click Overview.
5. To review access and error logs, click Logs.

   To choose which log to view, use the View pop-up menu.
6. To see graphs of connected users or throughput, click Graphs.

   Use the pop-up menus to choose which graph to view and to choose the duration of time to graph data for.
7. To see a list of connected users, click Connections.

   The list includes user name, connection status, user IP address or domain name, duration of connection, and the time since the last data transfer (idle time).

From the command line:

You can also check the status of the AFP service process by using the `ps` or `top` commands in Terminal, or by looking at the log files in /Library/Logs/AppleFileService/ using the `cat` or `tail` command.

- To view AFP service status:

```
$ sudo serveradmin status afp
```

- To see complete AFP status:

```
$ sudo serveradmin fullstatus afp
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing AFP Service Logs

Use Server Admin to view the error and access logs for AFP service, if you have enabled them.

To view logs:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Choose between access and error logs by clicking Logs, then use the View pop-up menu.

   Use the Filter field in the upper right to search for specific entries.

From the command line:

You can also view AFP service logs in /Library/Logs/AppleFileService/ using the `cat` or `tail` commands in Terminal.

- To view logs:

```
$ tail /Library/Logs/AppleFileService/
```

For information about `tail` and `cat`, see their man pages. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing AFP Graphs

Use Server Admin to view AFP graphs.

To view AFP graphs:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. To see graphs of connected users or throughput, click Graphs.

   To choose which graph to view and the duration of time to graph data for, use the pop-up menus.
5. To update the data in the graphs, click the Refresh button (below the Servers list).

Viewing AFP Connections

Use Server Admin to view the clients that are connected to the server through AFP service.

To view AFP connections:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. To see a list of connected users, click Connections.

   The list includes user name, connection status, user IP address or domain name, duration of connection, and the time since the last data transfer (idle time).

   You can send a stop message to client computers by clicking Stop (next to "Number of connections"), entering when the service will stop, entering a message, and clicking Stop.

   You can send a message to a user by selecting the user from the list, clicking Send Message, entering the message, and clicking Send.

   You can send a disconnect message to individual client computers and disconnect them from the server by clicking Disconnect, entering when the user will be disconnected, entering a message, and clicking Send.

   Important: Disconnected users can lose unsaved changes in open files.
5. To update the list of connected users, click the Refresh button (below the Servers list).

From the command line:

- To view AFP connections:

```
$ sudo serveradmin command afp:command = getConnectedUsers
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Stopping AFP Service

Use Server Admin to stop AFP service. This disconnects all users, so connected users might lose unsaved changes in open files.

To initiate AFP service shutdown and warn users:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.

4 Click Connections, then click Stop.

5 Enter the amount of time that users have to save their files before AFP service stops.

6 If you want users to know why they must disconnect, enter a message in the Additional Message field.

Otherwise, a default message is sent indicating that the server will shut down in the specified number of minutes.

7 Click Stop.

From the command line:

- To stop AFP service:

```
$ sudo serveradmin stop afp
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Enabling Bonjour Browsing for AFP Share Points

You can register AFP service with Bonjour to enable users to find the server by browsing through available servers. Otherwise, users who cannot browse must enter the server host name or IP address when connecting.

To register with Bonjour:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select AFP.

4 Click Settings, then click General.

5 Select "Enable Bonjour registration."

6 Click Save.

AFP share points use the Bonjour registration type `afpserver`.

From the command line:

- To register with Bonjour:

```
$ sudo serveradmin settings afp registerNSL = yes
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Limiting Connections to AFP Service

If your server provides a variety of services, you can prevent a flood of users from affecting the performance of those services by limiting the number of clients and guests who can connect at the same time.

To set the maximum number of connections:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Access and look under "Maximum Connections."

   By default the maximum client and guest connections is set to Unlimited.
5. Click the button next to the number field following "Client Connections (Including Guests)" and enter the maximum number of connections you want to permit.

   The guest connections limit is based on the client connections limit, and guest connections count as part of the total connection limit. For example, if you specify maximums of 400 client connections and 50 guest connections, and 50 guests are connected, that leaves 350 connections for registered users.

   The maximum number of simultaneous users is limited by the type of license you have. For example, if you have a 10-user license for your server, a maximum of 10 users can connect at one time.
6. Click the button next to the number fields and adjacent to "Guest connections" and enter the maximum number of guests you want to permit.

   Guest Connections is grayed out and cannot be edited until you select the "Enable Guest access" checkbox.
7. Click Save.

From the command line:

- To set the maximum number of connections:

```
$ sudo serveradmin settings afp:maxConnections = value
```

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Keeping an Access Log for AFP Service

The access log records the times when a user connects or disconnects, opens a file, or creates or deletes a file or folder.

To set up access logging:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Logging.
5. Select "Enable access log."
6. Select the events you want to record.

   When choosing events to log, consider available disk space. The more events you choose, the faster the log file will grow.

   To view the log, open Server Admin, select AFP, and click Logs. Alternatively, use Terminal to view the logs stored in /Library/Logs/AppleFileService/.
7. Click Save.

From the command line:

- To set up access logging:

```
$ sudo serveradmin settings
afp:activityLog = yes
afp:activityLogTime = value
afp:loggingAttributes:logLogin = value
afp:loggingAttributes:logLogout = value
afp:loggingAttributes:logOpenFork = value
afp:loggingAttributes:logCreateFile = value
afp:loggingAttributes:logCreateDir = value
afp:loggingAttributes:logDelete = value
afp:errorLogTime = 0
Control-D
```

Parameter	Description
`activityLog`	Turn activity logging on or off. Default = `no`
`loggingAttributes: logLogin`	Record user logins in the activity log. Default = `yes`
`loggingAttributes: logLogout`	Log user logouts in the activity log. Default = `yes`

Parameter	Description
`loggingAttributes: logOpenFork`	Log file opens in the activity log. Default = `yes`
`loggingAttributes: logCreateFile`	Record file creations in the activity log. Default = `yes`
`loggingAttributes: logCreateDir`	Record folder creations in the activity log. Default = `yes`
`loggingAttributes: logDelete`	Record file deletions in the activity log. Default = `yes`
`activityLogTime`	Rollover time (in days) for the activity log. Default = `7`

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Disconnecting a User from the AFP Server

Use Server Admin to disconnect users from the AFP server.

Important: Users lose information they haven't saved when they are disconnected.

To disconnect a user:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Connections.
5. Select the user and click Disconnect.
6. Enter the amount of time before the user is disconnected and provide a disconnect message.

   If you don't provide a message, a default message appears.
7. Click Disconnect.

From the command line:

- To set up access logging:

```
$ sudo serveradmin settings
afp:command = disconnectUsers
afp:message = "message-text"
afp:minutes = minutes-until
```

```
afp:sessionIDsArray:_array_index:0 = sessionid1
afp:sessionIDsArray:_array_index:1 = sessionid2
afp:sessionIDsArray:_array_index:2 = sessionid3
Control-D
```

Parameter	Description
message-text	The message that appears on client computers in the disconnect announcement dialog.
minutes-until	The number of minutes between the time the command is executed and the users are disconnected.
sessionidn	The session ID of a user you want to disconnect. To list the session IDs of connected users, use the `getConnectedUsers` command.

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Automatically Disconnecting Idle Users from the AFP Server

You can set AFP service to disconnect users who have not used the server for a period of time.

To set how the server handles idle users:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Idle Users.
5. To enable client computers to reconnect after sleeping, select "Allow clients to sleep __ hours" and enter the number of hours clients can sleep and still automatically reconnect to the server.

   Although the server disconnects sleeping clients, the clients' sessions are maintained for the specified period. When a user resumes work within that time, the client is reconnected with no apparent interruption.
6. To specify the idle time limit, select "Disconnect idle users after __ minutes" and enter the number of minutes after which an idle computer should be disconnected.

   A sleeping Mac OS X v10.2 (or later) client can resume work on open files within the limits of the "Allow clients to sleep" setting.
7. To prevent types of users from being disconnected, select them under "Except."

8 In the "Disconnect Message" field, enter the message you want users to see when they are disconnected.

If you don't enter a message, a default message appears stating that the user has been disconnected because the connection has been idle.

9 Click Save.

From the command line:

- To change AFP service Idle User settings:

```
$ sudo serveradmin settings
afp:clientSleepOnOff = value
afp:clientSleepTime = value
afp:idleDisconnectOnOff = value
afp:idleDisconnectTime = value
afp:idleDisconnectFlag:guestUsers = value
afp:idleDisconnectFlag:adminUsers = value
afp:idleDisconnectFlag:registeredUsers = value
afp:idleDisconnectFlag:usersWithOpenFiles = value
afp:idleDisconnectMsg = "value"
Control-D
```

Parameter	Description
`clientSleepOnOff`	Allow client computers to sleep. Default = `yes`
`clientSleepTime`	Time (in hours) that clients are allowed to sleep. Default = `24`
`idleDisconnectOnOff`	Enable idle disconnect. Default = `no`
`idleDisconnectTime`	Idle time (in minutes) allowed before disconnect. Default = `10`
`idleDisconnectFlag: guestUsers`	Enforce idle disconnect for guest users. Default = `yes`
`idleDisconnectFlag: adminUsers`	Enforce idle disconnect for administrator users. Default = `yes`
`idleDisconnectFlag: registeredUsers`	Enforce idle disconnect for registered users. Default = `yes`
`idleDisconnectFlag: usersWithOpenFiles`	Enforce idle disconnect for users with open files. Default = `yes`
`idleDisconnectMsg`	Idle disconnect message. Default = `""`

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Sending a Message to an AFP Service User

You can use AFP service in Server Admin to send messages to clients.

To send a user a message:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Connections and select the user's name in the list.
5. Click Send Message.
6. Enter the message and click Send.

   Note: Users cannot reply to the message.

From the command line:

- To send a user a message

```
$ sudo serveradmin command
afp:command = sendMessage
afp:message = "message-text"
afp:sessionIDsArray:_array_index:0 = sessionid1
afp:sessionIDsArray:_array_index:1 = sessionid2
afp:sessionIDsArray:_array_index:2 = sessionid3
[...]
Control-D
```

Parameter	Description
message-text	Message that appears on client computers.
sessionidn	Session ID of the user you want to receive the message. To list the session IDs of connected users, use the `getConnectedUsers` command.

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Enabling Guest Access to the AFP Server

Guests are users who can see information about your server without using a name or password to log in. For better security, don't permit guest access.

After enabling guest access for a service, enable guest access for specific share points. See "Enabling Guest Access to a Share Point" on page 58.

To enable guest access:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click Access.
5. Select "Enable Guest access."
6. If you want to limit how many client connections can be used by guests, enter a number in the "Maximum Connections: Guest Connections" option.

   If you don't want to limit the number of guest users who can be connected to your server at one time, select "Unlimited."
7. Click Save.

From the command line:

- To change several settings:

```
$ sudo serveradmin settings
afp:guestAccess = value
afp:maxConnections = value
afp:maxGuests = value
Control-D
```

Parameter	Description
`guestAccess`	Allow guest users access to the server. Default = `yes`
`maxConnections`	Maximum simultaneous user sessions allowed by the server. Default = `-1` (unlimited)
`maxGuests`	Maximum simultaneous guest users allowed. Default = `-1` (unlimited)

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Creating a Login Greeting for AFP Service

The login greeting is a message users see when they log in to the server.

To create a login greeting:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select AFP.
4. Click Settings, then click General.
5. In the Login Greeting field, enter a message.

   If you change the message, users see the new message the next time they connect to the server.
6. To prevent users from seeing the message more than once, select "Do not send same greeting twice to the same user."
7. Click Save.

From the command line:

- To create a login greeting:

```
$ sudo serveradmin settings
afp:loginGreeting = "value"
afp:loginGreetingTime = value
Control-D
```

Parameter	Description
`loginGreeting`	Login greeting message. Default = ""
`loginGreetingTime`	Last time the login greeting was set or updated.

For more information about command-line parameters for AFP, see "AFP Parameters" on page 141. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Integrating Active Directory and AFP Service

You can configure AFP service to use Active Directory for authenticating and authorizing Mac users to an AFP share point.

If you have a mixed platform environment with Windows and Mac computers you can integrate a Mac OS X AFP server with your Windows Active Directory server. Mac users can access the AFP share point by using their Active Directory user account credentials.

To integrate AFP with Active Directory:

1. Create an AFP share point for your Mac users.

   For more information, see "Creating a Share Point" on page 36.

2. Open System Preferences (located in /Applications/).
3. Click Accounts.
4. If the lock icon is locked, click it and enter the name and password for an administrator.
5. Click Login Options.
6. Click Directory Services, then click the Add (+) button.
7. From the "Add a new directory of type" pop-up menu, choose Active Directory, then enter the following information:
   - *Active Directory Domain:* This is the DNS name or IP address of the Active Directory server.
   - *Client Computer ID:* Optionally edit the ID you want Active Directory to use for your server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation.

     If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."
   - *AD Administrator Username and Password:* Enter the user name and password of the Active Directory administrator.
8. Click OK and then click Done.

Supporting AFP Clients

After you configure share point and AFP service, users can connect using the Connect to Server window in Finder or they can have the shared volume mount when they log in.

Note: Non-Apple clients can also connect over AFP using third-party AFP client software.

Mac OS X Clients

AFP service requires the following Mac OS X system software:

- TCP/IP connectivity
- AppleShare 3.7 or later

To find out the latest version of AppleShare client software supported by Mac OS X, go to the Apple support website at www.apple/support.

Connecting to the AFP Server in Mac OS X

You can connect to Apple file servers by entering the DNS name of the server or its IP address in the Connect to Server window. Or, if the server is registered with Bonjour browse for it in the Network globe in the Finder.

Note: Apple file service doesn't support AppleTalk connections, so clients must use TCP/IP to access file services.

To connect to the Apple file server in Mac OS X:

1. In the Finder, choose Go > Connect to Server.
2. In the Connect to Server pane, do one of the following:
   - Browse for the server in the list. If it appears, select it.
   - Enter the DNS name of the server in the Server Address field using any of the following forms:

     ```
     server

     afp://server

     afp://server/share point
     ```

   - Enter the server IP address in the Server Address field.
3. Click Connect.
4. Enter your user name and password or select Guest, then click Connect.
5. Select the share point you want to use and click OK.

Changing the Default User Name for AFP Connections

When you use the Connect to Server command in the Finder to connect to an AFP server, the login panel populates your full user name by default. In Mac OS X v10.5 and later, you can customize this panel to present your short name, a custom name, or no user name at all.

Important: These instructions involve using the `defaults` command to edit a property list (.plist) file and are intended for experienced Mac OS X administrators. Incorrect editing of this file can lead to unexpected Mac OS X behavior. Before following these instructions, make a backup copy of the /Library/Preferences/com.apple.NetworkAuthorization.plist file.

You can edit this file so that the Name field in the Connect to Server dialog is populated with one of the following:

- Current user's long name (default behavior)
- Current user's short name
- A custom name
- No name

Note: If you select the "Remember password in keychain" option in the Connect to Server dialog, the name stored in the Keychain entry overrides the setting in this preference file.

Use the `defaults` command in Terminal to change the default name to the following:

To set the current user's short name:

```
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseDefaultName -bool NO
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseShortName -bool YES
```

To set a custom name:

```
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseDefaultName -bool YES
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     DefaultName "user"
```

Replace `"user"` with the custom name and enclose it in quotation marks.

To set no name:

```
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseDefaultName -bool YES
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     DefaultName ""
```

To set the current user's long name:

This is only necessary if you have made any of the changes listed above.

```
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseDefaultName -bool NO
$ defaults write /Library/Preferences/com.apple.NetworkAuthorization
     UseShortName -bool NO
```

or

```
$ defaults delete /Library/Preferences/com.apple.NetworkAuthorization
     UseDefaultName
$ defaults delete /Library/Preferences/com.apple.NetworkAuthorization
     UseShortName
```

Setting Up a Mac OS X Client to Automatically Mount a Share Point

As an alternative to using the network mount feature of AFP or NFS, Mac OS X users can set their computers to automatically mount server volumes.

To set a Mac OS X v10.2.8 or earlier client to automatically mount a server volume:

1. Log in to the client computer as the user and mount the volume.
2. Open System Preferences and click Login Items.

3 Click Add, then locate the Recent Servers folder and double-click the volume you want automatically mounted.

When the user logs in the next time, the server, if available, mounts.

The user can also add the server volume to Favorites and then use the item in the Favorites folder in the home Library.

To set a Mac OS X v10.3 or later client to automatically mount a server volume:

1 Log in to the client computer as the user and mount the volume.

2 Open System Preferences and click Accounts.

3 Select the user and click Startup Items (in Mac OS X v10.3) or Login Items (in Mac OS X v10.4 or later).

4 Click the Add (+) button (below the Servers list), select the server volume, and click Add.

Connecting to the AFP Server from Mac OS 8 and Mac OS 9 Clients

AFP service requires the following Mac OS 8 or 9 system software:

- Mac OS 8 v8.6 or Mac OS 9 v9.2.2
- TCP/IP
- AppleShare Client 3.7 or later

To find the latest version of AppleShare client software supported by Mac OS 8 and Mac OS 9, go to the Apple support website at www.apple/support.

Note: AFP service does not support AppleTalk connections, so clients must use TCP/IP to access file services.

To connect from Mac OS 8 or Mac OS 9:

1 Open the Chooser and click AppleShare.

2 Select a file server and click OK.

3 Enter your user name and password, or select Guest and then click Connect.

4 Select the volume you want to use and click OK.

Setting up a Mac OS 8 or Mac OS 9 Client to Automatically Mount a Share Point

As an alternative to using the network mount feature of AFP or NFS, clients can set their computers to automatically mount server volumes.

To set a Mac OS 8 or Mac OS 9 client to automatically mount a server volume:

1 Use the Chooser to mount the volume on the client computer.

2 In the select-item dialog that appears after you log in, select the server volume you want to mount automatically.

Working with SMB Service

5

Use this chapter to set up and manage SMB service in Mac OS X Server.

Mac OS X Server can provide the following native services to Windows clients:

- **Domain login.** Enables each user to log in using the same user name, password, roaming profile, and network home folder on any Windows computer capable of logging in to a Windows NT domain.
- **File service.** Enables Windows clients to access files stored in share points on the server using Server Message Block (SMB) protocol over TCP/IP.
- **Print service.** Enables Windows clients to print to PostScript printers with print queues on the server.
- **Windows Internet Naming Service (WINS).** Enables clients to resolve NetBIOS names and IP addresses across multiple subnets.
- **Windows domain browsing.** Enables clients to browse for available servers across subnets.

File Locking with SMB Share Points

File locking prevents multiple clients from changing the same information at the same time. When a client opens a file (or part of a file), the file becomes locked so the client has exclusive access.

Before a read or write is performed on a file, the lock database is checked to verify the lock status of the file.

Strict locking, enabled by default, helps prevent multiple clients from attempting to write to the same file. When strict locking is enabled, the SMB server checks for and enforces file locks.

Opportunistic locking (oplocks) grants exclusive access to the file similarly to strict locking, but also permits the client to cache its changes locally (on the client computer). This type of locking offers improved performance.

In Mac OS X Server, SMB share points support oplocks.

To enable oplocks, change SMB protocol settings for a share point using Workgroup Manager. For more information, see "Changing SMB Settings for a Share Point" on page 40.

Important: Do not enable oplocks unless the share point is using only SMB. If the share point uses any other protocol, data can become corrupt.

Setup Overview

Here is an overview of the basic steps for setting up SMB service.

Step 1: Turn SMB service on Before configuring SMB service, SMB must be turned on. See "Turning On SMB Service" on page 96.

Step 2: Configure SMB General settings SMB General settings enable you to specify the number of authenticated and anonymous users that are permitted to connect to the server. See "Configuring SMB General Settings" on page 96.

Step 3: Configure SMB Access settings Access settings enable you to permit guest Windows users, limit the number of simultaneous Windows client connections, or set Windows authentication options. See "Configuring SMB Service Access Settings" on page 99.

Step 4: Configure SMB Logging settings Logging settings enable you to specify how much information is recorded in SMB log files. See "Configuring SMB Service Logging Settings" on page 101.

Step 5: Configure SMB Advanced settings Advanced settings enable you to choose a client code page, set the server to be a workgroup or domain master browser, specify the server WINS registration, and enable virtual share points for home users. See "Configuring SMB Service Advanced Settings" on page 102.

Step 6: Create share points and share them using SMB Use the Sharing service of Server Admin to specify the share points you want to make available through SMB. For Windows users to access a share point, you must explicitly configure the share point to use SMB service. See "Creating a Share Point" on page 36 and "Changing SMB Settings for a Share Point" on page 40.

You can also create virtual share points that enable each user to have the same home folder whether logging in from a Windows workstation or a Mac OS X computer. See "Enabling or Disabling Virtual Share Points" on page 107.

Step 7: Start SMB service After you configure SMB, start the services to make them available. See "Starting SMB Service" on page 104.

Turning On SMB Service

Before you can configure SMB settings, you must turn on SMB service.

To turn on SMB service:

1. Open Server Admin and connect to the server.
2. Click Settings, then click services.
3. Click the SMB checkbox.
4. Click Save.

Setting Up SMB Service

You set up SMB service by configuring four groups of settings on the Settings pane for SMB service in Server Admin:

- **General.** Specify the server's role in providing SMB service and the server's identity among clients of its SMB service.
- **Access.** Limit the number of clients and control guest access.
- **Logging.** Choose how much information is recorded in the service log.
- **Advanced.** Configure WINS registration and domain browsing services, choose a code page for clients, and control virtual share points for home folders.

Because the default settings work well if you want to provide only SMB file and print services, you may only need to start SMB service. Nonetheless, check the settings and change anything that is incorrect for your network.

To set up a Mac OS X Server as one of the following, you must change some settings:

- A Primary Domain Controller (PDC)
- A Backup Domain Controller (BDC)
- A member of the Windows domain of Mac OS X Server PDC
- A member of an Active Directory domain of a Windows server

In addition, your Windows client computers *must* be configured to access SMB service on Mac OS X Server as described at the end of this chapter, especially if users will log in to the Windows domain.

The following sections describe how to configure these settings and how to start SMB service.

Configuring SMB General Settings

Use the General settings to select the server role and provide the description, computer name, and workgroup for the server.

To configure SMB General settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings, then click General.
5. From the Role pop-up menu, set the Windows server role:
   - Choose "Standalone Server" if you want your server to provide SMB file and print services to users with accounts in the server local directory domain. The server will not provide authentication services for Windows domain login on Windows computers. This is the default.
   - Choose "Domain Member" if you want your server to provide Windows file and print services to users who log in to the Windows domain of a Mac OS X Server PDC or the Active Directory domain of a Windows server. A domain member can host user profiles and network home folders for user accounts on the PDC or the Active Directory domain.
   - Choose "Primary Domain Controller (PDC)" if you want your server to host a Windows domain, to store user, group, and computer records, and to provide authentication for domain login and other services. If no domain member server is available, the PDC server can provide Windows file and print services, and it can host user profiles and network home folders for users with user accounts on the PDC.
   - Choose "Backup Domain Controller (BDC)" if you want your server to provide automatic failover and backup for the Mac OS X Server PDC. The BDC handles authentication requests for domain login and other services as needed. The BDC can host user profiles and network home folders for user accounts on the PDC.

   Note: Mac OS X Server can host a PDC only if the server is an Open Directory master, and can host a BDC only if the server is an Open Directory replica. For information about Mac OS X Server directory and authentication services, including Open Directory master and replicas, see *Open Directory Administration*.
6. Enter a description, computer name, and domain or workgroup:
   - For Description, enter a description of the computer. This appears in the Network Places window on Windows computers, and is optional.
   - For Computer Name, enter the name you want Windows users to see when they connect to the server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."

- For Domain, enter the name of the Windows domain that the server will host. The domain name cannot exceed 15 characters and cannot be "workgroup."
- For Workgroup, enter a workgroup name. Windows users see the workgroup name in the My Network Place (or Network Neighborhood) window. If you have Windows domains on your subnet, use one of them as the workgroup name to make it easier for clients to communicate across subnets. Otherwise, consult your Windows network administrator for the correct name. The workgroup name cannot exceed 15 characters.

7 Click Save.

From the command line:

- To configure SMB General setting:

```
$ sudo serveradmin settings
smb:adminCommands:serverRole = value
smb:server string = value
smb:netbios name = value
smb:workgroup = value
Control-D
```

Parameter	Description
`adminCommands:serverRole`	The authentication role played by the server. Can be set to: • `standalone` • `domainmember` • `primarydomaincontroller` • `backupdomaincontroller` This corresponds to the Role pop-up menu in the General pane of Windows service settings in the Server Admin application.
`server string`	Text that helps identify the server in the network browsers of client computers. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the Description field in the General pane of the Windows service settings in the Server Admin application.
`netbios name`	The server's NetBIOS name. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the Computer Name field in the General pane of the Windows service settings in the Server Admin application.
`workgroup`	The server's workgroup. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the Workgroup field in the General pane of the Windows service settings in the Server Admin application.

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring SMB Service Access Settings

Use the Access pane of SMB service settings in Server Admin to permit anonymous Windows users or to limit the number of simultaneous Windows client connections. You can also select the kinds of authentication SMB service accepts.

To configure SMB service access settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings, then click Access.

5 To permit Windows or other SMB users to connect to Windows file services without providing a user name or password, select "Allow Guest access."

Guest access is a convenient way to provide occasional users with access to files and other items, but for better security, don't select this option.

6 To limit the number of users who can be connected to the SMB service at one time, select "__ maximum" and enter a number in the field.

7 Select the kinds of authentication Windows users can use.

Authentication options are NTLMv2 & Kerberos, NTLM, or LAN Manager. NTLMv2 & Kerberos is the most secure option, but clients need Windows NT, Windows 98, or later to use it. LAN Manager is the least secure, but Windows 95 clients can use it.

8 Click Save.

From the command line:

- To configure SMB service access settings:

```
$ sudo serveradmin settings
smb:map to guest = value
smb:max smbd processes = value
Control-D
```

Parameter	Description
`map to guest`	Whether guest access is allowed. Can be set to: • `"Never"` (No guest access) • `"Bad User"` (Allow guest access) This corresponds to the "Allow Guest access" checkbox in the Access pane of Windows service settings in the Server Admin application.
`max smbd processes`	The maximum allowed number of smbd server processes. Each connection uses its own smbd process, so this is the same as specifying the maximum number of SMB connections. `0` means unlimited. This corresponds to the "maximum" client connections field in the Access pane of the Windows service settings in the Server Admin application.

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring SMB Service Logging Settings

Use the Logging pane of SMB service settings in Server Admin to specify how much information is recorded in the SMB log file.

To configure the SMB service logging level:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings, then click Logging.
5. From the pop-up menu, set the level of log detail:
   - Choose "Low" to record error and warning messages only.
   - Choose "Medium" to record error and warning messages, service start and stop times, authentication failures, and browser name registrations.
   - Choose "High" to record error and warning messages, service start and stop times, authentication failures, browser name registrations, and file accesses.
6. Click Save.

From the command line:

- To configure SMB service access settings:

```
$ sudo serveradmin settings smb:log level = value
```

Parameter	Description
`log level`	The amount of detail written to the service logs. Can be set to: • `0` (Low: errors and warnings only) • `1` (Medium: service start and stop, authentication failures, browser name registrations, and errors and warnings) • `2` (High: service start and stop, authentication failures, browser name registration events, log file access, and errors and warnings) This corresponds to the Log Detail pop-up menu in the Logging pane of Windows service settings in the Server Admin application.

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring SMB Service Advanced Settings

Use the Advanced pane of SMB service settings in Server Admin to choose a client code page, set the server to be a workgroup or domain master browser, specify the server's WINS registration, and enable virtual share points for user homes.

To configure SMB service Advanced settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings, then click Advanced.
5. From the Code Page pop-up menu, choose the character set you want clients to use.
6. Select how you want the server to perform discovery and browsing services:
   - To provide discovery and browsing of servers in a single subnet, select "Services: Workgroup Master Browser."
   - To provide discovery and browsing of servers across subnets, select "Services: Domain Master Browser."
7. Select how you want the server to register with WINS:
   - To prevent your server from using or providing WINS for NetBIOS name resolution, select "Off."
   - To enable your server to provide NetBIOS name resolution service, select "Enable WINS server." This feature enables clients across multiple subnets to perform name and address resolution.
   - To enable your server to use an existing WINS service for NetBIOS name resolution, select "Register with WINS server" and enter the IP address or DNS name of the WINS server.
8. Select whether you want virtual share points to be enabled:
   - If you enable virtual share points, each user has the same network home folder whether they log in from a Windows workstation or a Mac OS X computer.
   - If you disable virtual share points, you must set up an SMB share point for Windows home folders and you must configure each Windows user account to use this share point.
9. Click Save.

From the command line:

- To configure SMB service access settings:

```
$ sudo serveradmin settings
smb:dos charset = value
smb:domain master = value
```

```
smb:local master = value
smb:wins support = value
smb:wins server = value
Control-D
```

Parameter	Description
`dos charset`	The code page being used. Can be set to: • `437` (Latin US) • `737` (Greek) • `775` (Baltic) • `850` (Latin1) • `852` (Latin2) • `861` (Icelandic) • `866` (Cyrillic) • `932` (Japanese SJIS) • `936` (Simplified Chinese) • `949` (Korean Hangul) • `950` (Traditional Chinese) • `1251` (Windows Cyrillic) This corresponds to the Code Page pop-up menu on the Advanced pane of Windows service settings in the Server Admin application.
`domain master`	Whether the server is providing Windows domain master browser service. Can be set to: `yes | no` This corresponds to the Domain Master Browser checkbox in the Advanced pane of Windows service settings in the Server Admin application.
`local master`	Whether the server is providing Windows workgroup master browser service. Can be set to: `yes | no` This corresponds to the Workgroup Master Browser checkbox in the Advanced pane of Windows service settings in the Server Admin application.

Parameter	Description
`wins support`	Whether the server provides WINS support. Can be set to: `yes | no` This corresponds to the WINS Registration "Off" and "Enable WINS" server options in the Advanced pane of the Windows service settings in the Server Admin application.
`wins server`	The name of the WINS server used by the server. This corresponds to the WINS Registration "Register with WINS server" option and field in the Advanced pane of the Windows service settings in the Server Admin application.

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Starting SMB Service

You start SMB service to make it available to users.

To start SMB service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Start SMB (below the Servers list).

From the command line:

- To start SMB service:

```
$ sudo serveradmin start smb
```

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Managing SMB Service

This section describes typical tasks you might perform after you set up SMB service on your server. Initial setup information appears in "Setting Up SMB Service" on page 96.

Viewing SMB Service Status

Use Server Admin to view the status of SMB service.

To view SMB service status:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. To see whether the service is running, when it started, the number of connections, and whether guest access is enabled, click Overview.
5. To review the event log, click Logs.

   Use the View pop-up menu to choose which logs to view.
6. To see a graph of connected users, click Graphs.

   Use the pop-up menu to choose the duration to graph data for.
7. To see a list of connected users, click Connections.

   The list includes the user name, the user's IP address or domain name, and the duration of connection.

From the command line:

You can also view the status of the SMB service process using the `ps` or `top` commands in Terminal. To view the log files (located in /Library/Logs/WindowsServices/), use the `cat` or `tail` command.

- To view SMB service status:

```
$ sudo serveradmin settings status smb
```

- To view complete SMB service status:

```
$ sudo serveradmin settings fullstatus smb
```

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing SMB Service Logs

Use Server Admin to view SMB service logs.

To view SMB logs:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.

3 From the expanded Servers list, select SMB.

4 Click Logs and use the View pop-up menu to choose between "SMB File Service Log" and "SMB Name Service Log."

To choose the types of events that are recorded, see "Configuring SMB Service Logging Settings" on page 101.

From the command line:

- To view SMB logs:

```
$ tail log-filesudo serveradmin settings fullstatus smb
```

- To view the SMB service log and name service log paths:

```
$ sudo serveradmin command smb:command = getLogPaths
```

For information about `tail` or `serveradmin`, see their man pages. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing SMB Graphs

You use Server Admin to view SMB graphs.

To view SMB graphs:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select SMB.

4 To see a graph of average connected user's throughput over a period of time, click Graphs.

To choose the duration of time to graph data for, use the pop-up menu.

5 Update the data in the graph by clicking the Refresh button (below the Servers list).

Viewing SMB Connections

Use Server Admin to view the clients that are connected to the server through SMB service.

To view SMB connections:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select SMB.

4 To see a list of connected users, click Connections.

The list includes the user name, user IP address or domain name, and the duration of connection.

You can disconnect individual clients by selecting the user from the Connections list, clicking Disconnect, and then clicking Send.

Important: Disconnected users might lose unsaved changes in open files.

5 Update the list of connected users by clicking the Refresh button (below the Servers list).

From the command line:

- To view connected user information:

```
$ sudo serveradmin command smb:command = getConnectedUsers
```

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Stopping SMB Service

You stop SMB service using Server Admin.

Important: When you stop SMB service, users that are connected might lose unsaved changes in open files.

To stop SMB service:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select SMB.

4 Click Stop SMB (below the Servers list).

5 Click Stop Now.

From the command line:

- To view connected user information:

```
$ sudo serveradmin stop smb
```

For more information about command-line parameters for SMB, see "SMB Parameters" on page 148. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Enabling or Disabling Virtual Share Points

Using Server Admin, you can control whether Mac OS X Server creates a virtual SMB share point that maps to the share point selected for each user in Server Admin. This simplifies setting up home folders for Windows users by using the same home folder for Windows and Mac OS X.

If you enable virtual share points, each user has the same network home folder whether logging in from a Windows workstation or a Mac OS X computer.

If you disable virtual share points, you must set up an SMB share point for Windows home folders, and you must configure each Windows user account to use this share point.

To enable or disable virtual SMB share points for Windows home folders:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select SMB.
4. Click Settings, then click Advanced.
5. Click "Homes: Enable virtual share points."
6. Click Save.

Working with NFS Service

6

Use this chapter to learn how to set up and manage NFS Service in Mac OS X Server.

Network File System (NFS) is the protocol used for file services on UNIX computers. Use NFS service in Mac OS X Server to provide file services for UNIX clients (including Mac OS X clients).

You can share a volume (or export it, in standard NFS terminology) to a set of client computers or to "World." Exporting an NFS volume to World means that anyone who accesses your server can also access that volume.

NFS service supports POSIX file permissions. NFS does not support reading or changing Access Control List (ACL) permissions. ACLs are enforced by the file system exported by NFS.

Setup Overview

Here is an overview of the major steps for setting up NFS service.

Step 1: Before you begin For issues to keep in mind when you set up NFS service, read "Before Setting Up NFS Service" on page 110.

Step 2: Turn NFS service on Before configuring NFS service, turn on NFS. See "Turning On NFS Service" on page 110.

Step 3: Configure NFS settings Configure NFS settings to set the maximum number of daemons and choose how to serve clients—using Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or both. See "Configuring NFS Service Settings" on page 110.

Step 4: Create share points and share them using NFS Use the Sharing service of Server Admin to specify the share points you want to export (share) using NFS. For NFS users to access the share point, you must explicitly configure a share point to use NFS.

See "Creating a Share Point" on page 36, "Exporting an NFS Share Point" on page 43, and "Automatically Mounting Share Points for Clients" on page 46.

When you export a share point, NFS service starts. When you delete exports, NFS service stops. To see if NFS service is running, open Server Admin, select NFS from the list of services for your server, and click Overview.

Before Setting Up NFS Service

Mac OS X v10.5 and later offers NFS with Kerberos, providing another secure file sharing service. Secure access to NFS shared items is controlled by Kerberos, the client software, and file permissions. NFS with Kerberos can be configured to only grant access to shared volumes based on the IP address of a computer and a user's single sign-on credentials.

If your network has Mac OS X v10.4 and Mac OS X v10.6 computers, you can permit authentication through system authentication and Kerberos (by setting the Minimum Security option to Any) and then export your NFS share to World. This requires users in a Kerberos realm to get a ticket-granting ticket from a single sign-on Kerberos server before accessing NFS shared volumes, and still permits Mac OS X v10.4 computers to access the NFS share point using system authentication.

If your network has only Mac OS X v10.6 computers, it is recommended that you set the security to Kerberos authorization only.

Using NFS with Kerberos is the recommended way to configure secure access to files.

Turning On NFS Service

Before you can configure NFS settings, you must turn on NFS service in Server Admin.

To turn on NFS service:

1. Open Server Admin and connect to the server.
2. Click Settings, then click services.
3. Select the NFS checkbox.
4. Click Save.

Setting Up NFS Service

Use Server Admin to change NFS service settings. The following sections describe the tasks for configuring and starting NFS service.

Configuring NFS Service Settings

NFS service settings enable you to set the maximum number of daemons and choose how you want to serve clients—using TCP, UDP, or both.

To configure NFS service settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select NFS.
4. Click Settings.
5. In the "Use__server threads" field, enter the maximum number of NFS threads you want to run at one time.

   An NFS thread is a thread running inside the nfsd process. It continuously runs behind the scenes and processes read and write requests from clients. The more threads that are available, the more concurrent clients can be served.
6. Select how you want to serve data to your client computers.

   TCP separates data into packets (small bits of data sent over the network using IP) and uses error correction to make sure information is transmitted properly.

   UDP is a correctionless and connectionless transport protocol. UDP doesn't break data into packets, so it uses fewer system resources. It's more scalable than TCP and is a good choice for a heavily used server because it puts a smaller load on the server. However, do not use UDP if remote clients are using the service.

   TCP provides better performance for clients than UDP. However, unless you have a specific performance concern, select both TCP and UDP.
7. Click Save.

From the command line:

You can view or configure NFS service settings using the `serveradmin` command. You can configure the number of daemons you want to run at one time and whether you want to use TCP or UDP.

- To view a setting:

```
$ sudo serveradmin settings nfs:setting
```

- To view all settings:

```
$ sudo serveradmin settings nfs
```

- To change NFS service settings:

```
$ sudo serveradmin settings
nfs:nbDaemons = value
nfs:useTCP = value
nfs:useUDP = value
Control-D
```

Parameter (`nfs.`)	Description
`nbDaemons`	To reduce the number of daemons, restart the server after changing this value. Default = `6`.
`useTCP`	Restart the server after changing this value. Default = `yes`.
`useUDP`	Restart the server after changing this value. Default = `yes`.

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Starting NFS Service

You start NFS service to make NFS exports available to users.

To start NFS service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select NFS.
4. Click Start NFS (below the Servers list).

   The service runs until you stop it. It restarts if your server is restarted.

Managing NFS Service

Use Server Admin to manage NFS service settings.

Checking NFS Service Status

Use Server Admin to check the status of Mac OS X Server devices and services.

To view NFS service status:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select NFS.
4. Click Overview.

   The Overview pane tells you whether the service is running and whether nfsd, portmap, rpc.lockd, and rpc.statd processes are running.

The nfsd process responds to NFS protocol and mount protocol requests from client computers that have mounted folders.

The portmap process enables client computers to find nfs daemons (always one process).

The rpc.lockd daemon provides file and record-locking services in an NFS environment.

The rpc.statd daemon cooperates with rpc.statd daemons on other hosts to provide a status monitoring service. If a local NFS service quits unexpectedly and restarts, the local rpc.statd daemon notifies the hosts being monitored at the time the service quit.

5 To see a list of connected users, click Connections.

The list includes the user name, the user IP address or domain name, the time since the last data transfer (idle time), NFS requests, and the bytes read and written.

From the command line:

- To see if the service and related processes are running:

```
$ sudo serveradmin status nfs
```

- To see complete status:

```
$ sudo serveradmin fullstatus nfs
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing NFS Connections

Use Server Admin to view the active clients that are connected to the server through NFS service.

To view NFS connections:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select NFS.

4 To see a list of active users, click Connections.

The list includes the user name, the user IP address or domain name, the time since the last data transfer (idle time), NFS requests, and the bytes read and written.

5 To update the list of connected users, click the Refresh button (below the Servers list).

Stopping NFS Service

Use Server Admin to stop NFS service and disconnect users. Users who are connected when you stop NFS service might lose unsaved changes in open files.

To stop NFS service after warning users:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select NFS.
4. Click Connections, then see if users are connected to an NFS shared volume.

   If you stop the service while users are connected, your connected users might lose unsaved data.
5. Click Stop NFS.
6. Click Stop Now.

From the command line:

- You can also stop NFS service immediately using the `serveradmin` command in Terminal.

  For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing Current NFS Exports

Use the Terminal application to view a list of current NFS exports.

To view current NFS exports:

1. Open Terminal.
2. Enter the following command to display NFS exports:

   ```
   $ showmount -e
   ```

   If this command does not return results in a few seconds, there are no exports and the process does not respond.
3. Quit Terminal.

   Press Control-C to exit the `showmount` command and return to an active command line in your Terminal window.

Working with FTP Service

7

Use this chapter to set up and manage FTP Service in Mac OS X Server.

File Transfer Protocol (FTP) is a simple way for computers of any type to transfer files over the Internet. Someone using a computer that supports FTP or an FTP client application can connect to your FTP server and upload or download files, depending on the permissions you set.

Most Internet browsers and a number of freeware and shareware applications can be used to access your FTP server.

In Mac OS X Server, FTP service is based on the source code for Washington University's FTP server, known as "wu-FTPd." However, the original source code has been extensively modified to provide a better user experience. Some of the differences are described in the following sections.

A Secure FTP Environment

Most FTP servers restrict users to specific folders on the server. Users see content only in these directories, so the server is kept quite secure. Users cannot access volumes mounted outside the restricted folders, and symbolic links and aliases cannot reach outside these boundaries.

In Mac OS X Server, FTP service expands the restricted environment to permit access to symbolic links while still providing a secure FTP environment. You can permit FTP users to have access to the FTP root folder, their home folder, or to any other folder on the server that you set up as an FTP share point.

A user's access to the FTP root folder, FTP share points, and his or her home folder is determined by the user environment you specify (as described in the following section) and by access privileges.

Note: FTP service enforces ACL permissions.

FTP Users

FTP supports two types of users:

- **Authenticated users.** These users have accounts on your server, and might have home folders stored on the server. Some FTP software refers to these as *real* users. An authenticated user must provide a user name and password to access server files using FTP.

  You review or set up authenticated users using the Accounts module of Workgroup Manager.

- **Anonymous users.** These users do not have accounts on your server. They are also known as *guest* users (for example, when you set up an FTP share point in Server Admin). An anonymous user can access FTP folders on the server using the common user name "anonymous" and a fictitious mail address as their password.

  You permit anonymous access to your server using the General pane of the FTP service settings in Server Admin. See "Configuring FTP General Settings" on page 122.

The FTP Root Folder

The FTP root folder (or FTP root) is a portion of the disk space of your server set aside for FTP users. The FTP root is set to /Library/FTPServer/FTPRoot/ when you install the server software.

You can change the FTP root. See "Changing the FTP Root Folder" on page 131.

FTP User Environments

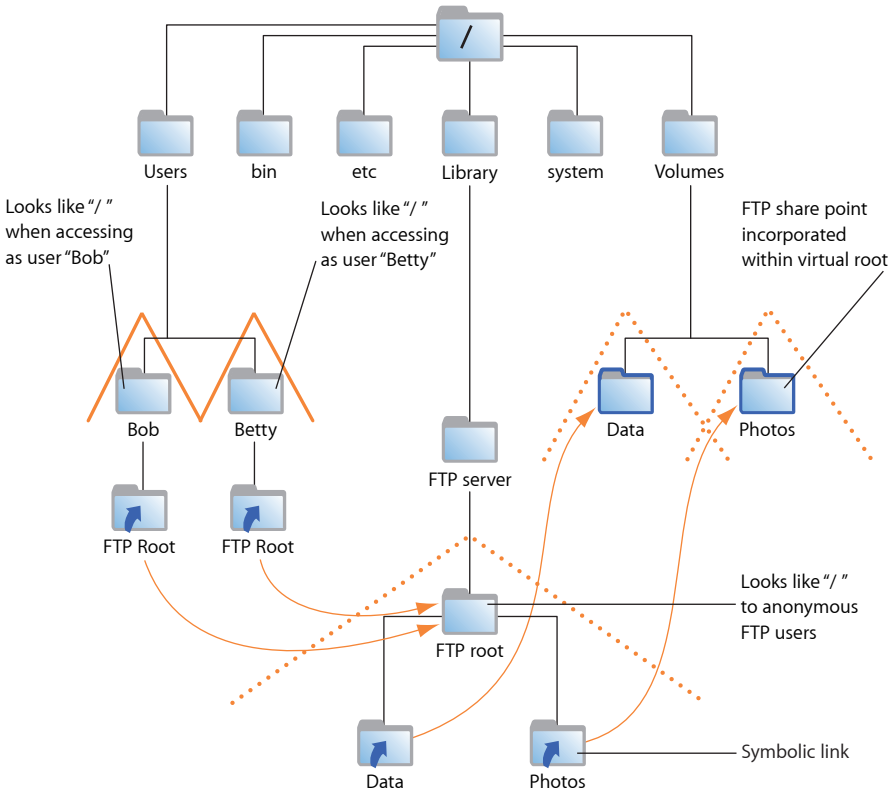
Mac OS X Server has three FTP environments to choose from:

- FTP root and Share Points
- Home Folder with Share Points
- Home Folder Only

To choose the user environment for your server, you use the Advanced pane of FTP service settings in Server Admin. For more information, see "Configuring FTP Advanced Settings" on page 128.

FTP Root and Share Points

The "FTP Root and Share Points" environment option gives access to the FTP root and any FTP share points that users have access privileges to, as shown in the following illustration.



Users access FTP share points through symbolic links attached to the FTP root folder. The symbolic links are created when you create FTP share points.

In this example, /Users, /Volumes/Data/, and /Volumes/Photos/ are FTP share points. All users can see the home folders of other users because they are subfolders of the Users share point.

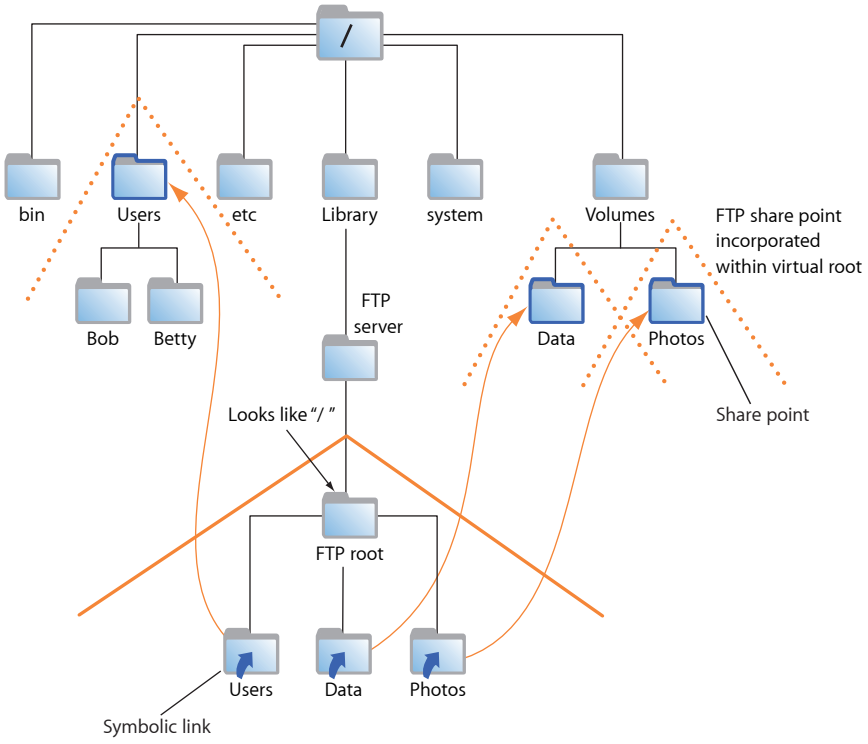
Important: Regardless of the user environment setting, anonymous users and users without home folders are always logged in to the FTP Root and Share Points environment.

Home Folder with Share Points

When the user environment option is set to "Home Folder with Share Points," authenticated users log in to their home folders and have access to the FTP root by a symbolic link created in their home folders.

Users access other FTP share points through symbolic links in the FTP root. As always, access to FTP share points is controlled by user access privileges.

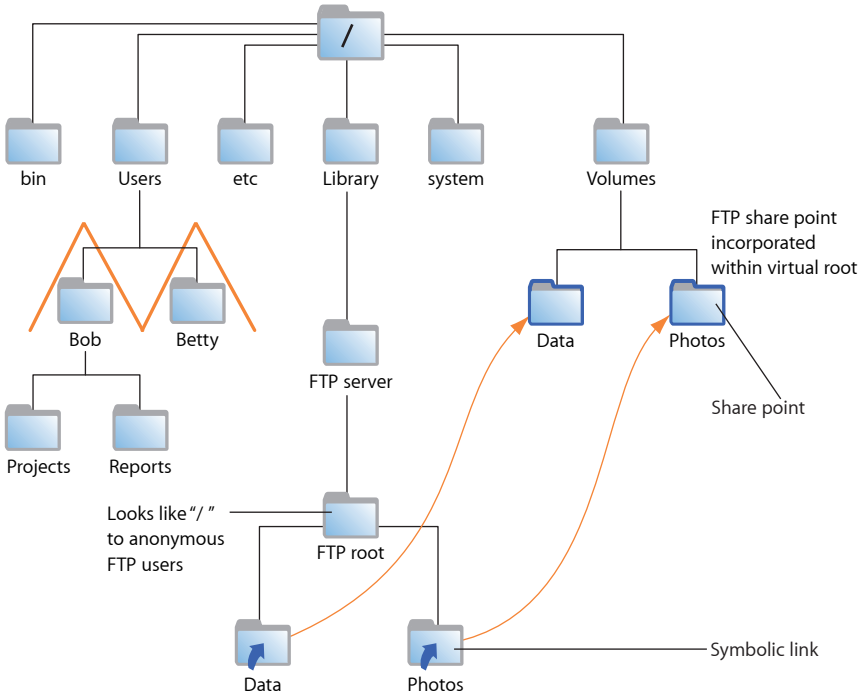
For users to access their home folders, the share point where the folders reside must be configured to be shared using FTP, as shown in the following illustration:



If you change the FTP root, the symbolic link in a user's home folder reflects that change. For example, if you change the FTP root to /Volumes/Extra/NewRoot/, the symbolic link created in the user's home folder is named NewRoot.

Home Folder Only

When you choose the "Home Folder Only" option, authenticated users are confined to their home folders and do not have access to the FTP root or other FTP share points, as shown in the following illustration:



Anonymous users and users without home folders still have access to the FTP root but cannot browse FTP share points.

On-the-Fly File Conversion

FTP service in Mac OS X Server enables users to request compressed or decompressed versions of information about the server.

A file-name suffix such as ".Z" or ".gz" indicates that the file is compressed. If a user requests a file named "Hamlet.txt" and the server only has a file named "Hamlet.txt.Z," the server knows that the user wants the decompressed version, and delivers it to the user in that format.

In addition to standard file compression formats, FTP in Mac OS X Server can read files from Hierarchical File System (HFS) or non-HFS volumes and convert the files to MacBinary (.bin) format. MacBinary is one of the most commonly used file compression formats for the Macintosh operating system.

The following table shows common file extensions and the type of compression they designate.

File extension	What it means
.gz	DEFLATE compression
.Z	UNIX compress
.bin	MacBinary encoding
.tar	UNIX tar archive
.tZ	UNIX compressed tar archive
.tar.Z	UNIX compressed tar archive
.crc	UNIX checksum file
.dmg	Mac OS X disk image

Files with Resource Forks

Mac OS X clients can take advantage of on-the-fly conversion to transfer files created using older file systems that store information in resource forks.

If you enable MacBinary and disk image autoconversion in FTP service settings, files with resource forks are listed as .bin files on FTP clients. When a client asks to have one of these files transferred, on-the-fly conversion recognizes the .bin suffix and converts the file to a genuine .bin file for transfer.

Kerberos Authentication

FTP supports Kerberos authentication. You choose the authentication method using the General pane of FTP service settings in Server Admin. See "Configuring FTP General Settings" on page 122.

FTP Service Specifications

FTP service has the following default specifications:

- Maximum authenticated users: 50
- Maximum anonymous users: 50
- Maximum connected users: 1000
- FTP port number: 21
- Number of failed login attempts before user is disconnected: 3

Setup Overview

Here is an overview of the basic steps for setting up FTP service.

Step 1: Before you begin For issues to keep in mind when you set up FTP service, read "Before Setting Up FTP Service" on page 121.

Step 2: Turn on FTP service Before configuring FTP service, FTP must be turned on. See "Turning On FTP Service" on page 122.

Step 3: Configure FTP General settings General settings enable you to specify the number of authenticated and anonymous users that can connect to the server, limit the number of login attempts, and provide an administrator address. See "Configuring FTP General Settings" on page 122.

Step 4: Configure FTP Messages settings Messages settings enable you to display banner and welcome messages, set the number of login attempts, and provide an administrator address. See "Configuring FTP Greeting Messages" on page 124.

Step 5: Configure FTP Logging settings Logging settings enable you to specify the FTP-related events you want to log for authenticated and anonymous users. See "Configuring FTP Logging Settings" on page 127.

Step 6: Configure FTP Advanced settings Advanced settings enable you to change the FTP root and choose which items users can see. See "Configuring FTP Advanced Settings" on page 128.

Step 7: Create an uploads folder for anonymous users If you enabled anonymous access in Step 2, you might want to create a folder for anonymous users to upload files. The folder must be named "uploads." It is not a share point but must have correct access privileges. See "Creating an FTP Uploads Folder for Anonymous Users" on page 130.

Step 8: Create share points and share them using FTP Use the Sharing service of Server Admin to specify the share points that you want to make available through FTP. You must explicitly configure a share point to use FTP so that FTP users can access the share point. See "Creating a Share Point" on page 36 and "Changing FTP Settings for a Share Point" on page 42.

Step 9: Start FTP service After you configure FTP service, start the service to make it available. See "Starting FTP Service" on page 129.

Before Setting Up FTP Service

When determining whether to offer FTP service, consider the type of information you will share and who your clients are. FTP works well when you want to transfer large files such as applications and databases. In addition, if you want to permit guest (anonymous) users to download files, FTP is a secure way to provide this service.

Server Security and Anonymous Users

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

The default settings for FTP prevent anonymous users from performing the following actions:

- Deleting files
- Renaming files
- Overwriting files
- Changing permissions of files

Anonymous FTP users are permitted only to upload files to a special folder named "uploads" in the FTP root. If the uploads folder doesn't exist, anonymous users can't upload files.

Turning On FTP Service

Before you can configure FTP settings, you must turn on FTP service in Server Admin.

To turn on FTP service:

1. Open Server Admin and connect to the server.
2. Click Settings, then click services.
3. Click the FTP checkbox.
4. Click Save.

Setting Up FTP Service

There are four groups of settings on the Settings pane for FTP service in Server Admin:

- **General.** Use to set information about access, file conversion, and login attempts for FTP service.
- **Messages.** Use to configure messages that appear to clients using FTP service.
- **Logging.** Use to configure and manage logs for FTP service.
- **Advanced.** Use to configure and administer advanced settings.

The following sections describe how to configure these settings, and how to start FTP service when you finish.

Configuring FTP General Settings

You can use the General settings to limit the number of login attempts, provide an administrator address, and limit the number and type of users.

To configure FTP General settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.

3. From the expanded Servers list, select FTP.
4. Click Settings, then click General.
5. To indicate the number of times users can try to connect before they are disconnected, enter a number in "Disconnect client after __ login failures."
6. To provide a contact for your users, enter a mail address in the "FTP administrator email address" field.
7. From the Authentication pop-up menu, choose an authentication method.
8. To limit the number of authenticated users who can connect to your server at the same time, enter a number in the "Allow a maximum of __ authenticated users" field.

   Authenticated users have accounts on the server. You can view or add them using the Accounts module of Workgroup Manager.
9. To permit anonymous users to connect to the server, select "Enable anonymous access."

   Important: Before selecting this option, review the privileges assigned to your share points under File Privileges in the Sharing pane to make sure there are no security holes.

   Anonymous users can log in using the name "ftp" or "anonymous." They do not need a password to log in, but they are prompted to enter their mail addresses.
10. To limit the number of anonymous users who can connect to your server at the same time, enter a number in the "Allow a maximum of __ anonymous users" field.
11. If you want to have files that have resource forks listed with a .bin suffix so that clients can take advantage of automatic file conversion when transferring them, select "Enable MacBinary and disk image auto-conversion."
12. Click Save.

From the command line:
You can view or configure the FTP service settings using the `serveradmin` command.

- To view a setting:

```
$ sudo serveradmin settings ftp:setting
```

- To view all settings:

```
$ sudo serveradmin settings ftp
```

- To view a group of settings:

  You can view a group of settings that have part of their names in common by entering as much of the name as you want, stopping at a colon (:), and entering an asterisk (*) as a wild card for the remaining parts of the name. For example:

```
$ sudo serveradmin settings ftp:logCommands:*
```

- To change FTP service settings:

```
$ sudo serveradmin settings
```

```
ftp:loginFailuresPermitted = value
ftp:administratorEmailAddress = value
ftp:authLevel = value
ftp:maxRealUsers = value
ftp:anonymousAccessPermitted = value
ftp:maxAnonymousUsers = value
ftp:enableMacBinAndDmgAutoConversion = value
Control-D
```

Parameter (`ftp:`)	Description
`administratorEmailAddress`	Sets the administrator mail address. Default = "`user@hostname`"
`anonymousAccessPermitted`	Allows anonymous access to FTP if you change the default setting to yes. Default = `no`
`authLevel`	Sets the authentication method. "`KERBEROS`" and "`ANY METHOD`" are the other possible values. Default = "`STANDARD`"
`enableMacBinAndDmgAutoConversion`	Default = `yes`
`loginFailuresPermitted`	Default = `3`
`maxAnonymousUsers`	Default = `50`
`maxRealUsers`	Default = `50`

For information about command-line parameters for FTP, see "FTP Parameters" on page 146. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring FTP Greeting Messages

Users see the banner message when they first contact your server (before they log in), and then they see the welcome message when they log in.

To change banner and welcome messages:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click Messages.

   The Messages pane appears, displaying the current text for both messages.
5. Edit the text.
6. Select "Show welcome message" and "Show banner message."

7 Click Save.

From the command line:

- To change the message and display settings:

```
$ sudo serveradmin settings
ftp:bannerMessage = "value"
ftp:welcomeMessage = "value"
ftp:showBannerMessage = value
ftp:showWelcomeMessage = value
Control-D
```

Parameter (`ftp.`)	Description
`bannerMessage`	Displays a banner message that appears when you are prompted to log in to FTP. Customize to your own preferences. Default ="----------This is the "Banner" message for the Mac OS X Server's FTP server process. FTP clients will receive this message immediately before being prompted for a name and password. PLEASE NOTE: Some FTP clients may exhibit problems if you make this file too long. ----------"
`welcomeMessage`	Displays a welcome message that appears after you log in to FTP. Customize to your own preferences. Default = "----------This is the "Welcome" message for the Mac OS X Server's FTP server process. FTP clients will receive this message right after a successful log in. ----------"
`showBannerMessage`	Default = `yes`
`showWelcomeMessage`	Default = `yes`

For information about command-line parameters for FTP, see "FTP Parameters" on page 146. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Displaying FTP Banner and Welcome Messages

FTP service in Mac OS X Server lets you greet users who contact or log in to your server.

Note: Some FTP clients might not display the message in an obvious place, or they might not display it at all. For example, in recent releases of the FTP client Fetch, you set a preference to display server messages.

The banner message appears when a user contacts the server, before they log in. The welcome message appears after they successfully log in.

To display banner and welcome messages to users:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click Messages.
5. Select "Show welcome message."
6. Select "Show banner message."
7. Click Save.

From the command line:

- To change display settings:

```
$ sudo serveradmin settings
ftp:showBannerMessage = value
ftp:showWelcomeMessage = value
Control-D
```

Parameter (`ftp:`)	Description
`showBannerMessage`	Default = `yes`
`showWelcomeMessage`	Default = `yes`

For information about command-line parameters for FTP, see "FTP Parameters" on page 146. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Displaying FTP Messages Using message.txt Files

If an FTP user opens a folder on your server that contains a file named "message.txt," the file contents appear as a message.

The user sees the message only the first time they connect to the folder during an FTP session. You can use the message to notify users of important information or changes.

Using FTP README Messages

If you place a file named README in a folder, an FTP user who opens that folder receives a message letting them know that the file exists and when it was last updated. The user can then choose to open and read the file.

Configuring FTP Logging Settings

Logging settings enable you to choose which FTP-related events to record.

For authenticated or anonymous users, you can record:

- Uploads
- Downloads
- FTP commands
- Rule violation attempts

To configure FTP Logging settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click Logging.
5. In the FTP log for anonymous users in the "Log Anonymous Users" section, select events you want to record.
6. In the FTP log for authenticated users in the "Log Authenticated Users" section, select events you want to record.
7. Click Save.

   To view the log, select FTP in Server Admin and click Log.

From the command line:

- To configure FTP log settings:

```
$ sudo serveradmin settings
ftp:logCommands:anonymous = value
ftp:logCommands:real = value
ftp:logSecurity:anonymous = value
ftp:logSecurity:real = value
ftp:logTransfers:anonymous:inbound = value
ftp:logTransfers:anonymous:outbound = value
ftp:logTransfers:real:inbound = value
ftp:logTransfers:real:outbound = value
Control-D
```

Parameter (`ftp.`)	Description
`logCommands:anonymous`	Default = `no`
`logCommands:real`	Default = `no`
`logSecurity:anonymous`	Default = `no`
`logSecurity:real`	Default = `no`
`logTransfers:anonymous:inbound`	Default = `yes`
`logTransfers:anonymous:outbound`	Default = `yes`
`logTransfers:real:inbound`	Default = `yes`
`logTransfers:real:outbound`	Default = `yes`

For information about command-line parameters for FTP, see "FTP Parameters" on page 146. For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Configuring FTP Advanced Settings

Advanced settings enable you to change the FTP root folder and to specify folders that authenticated FTP users can access.

To configure FTP Advanced settings:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click Advanced.
5. For "Authenticated users see," choose the type of user environment you want to use: FTP Root with Share Points, Home Folder with Share Points, or Home Folder Only.

   For more information, see "FTP Users" on page 116.
6. To change the FTP root, enter the new pathname in the FTP root field, or click Choose to select the new folder.

   For more information, see "The FTP Root Folder" on page 116.

From the command line:

You can also change the directory where the FTP content is stored using the `serveradmin` command. By default, the directory is /Library/FTPServer/FTPRoot.

- To change where the FTP content is stored:

```
$ sudo serveradmin settings ftp:ftpRoot = "value"
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Starting FTP Service

You must start FTP service to make it available to users.

To start FTP service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Start FTP (below the Servers list).

From the command line:

- To start FTP service:

```
$ sudo serveradmin start ftp
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Permitting Anonymous FTP User Access

You can permit guests to log in to your FTP server with the user name "ftp" or "anonymous." Guests don't need a password to log in, but they are prompted to enter a mail address.

For better security, do not enable anonymous access.

To enable anonymous FTP service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click General.
5. Under Access, select "Enable anonymous access."

   The default limit is 50.
6. Click Save.

From the command line:

- To enable anonymous FTP access:

```
$ sudo serveradmin settings ftp:anonymousAccessPermitted = yes
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Creating an FTP Uploads Folder for Anonymous Users

The uploads folder provides a place for anonymous users to upload files to the FTP server. It must exist at the top level of the FTP root folder and be named "uploads." If you change the FTP root folder, the uploads folder must also be changed.

To create an uploads folder for anonymous users:

1. Use the Finder to create a folder named "uploads" at the top level of your server FTP root folder.
2. Set privileges for the folder to permit guest users to write to it.

From the command line:

You can also set up an FTP upload folder using the `mkdir` and `chmod` commands in Terminal.

1. Create a folder named "uploads" at the top level of your server FTP root folder:

```
$ sudo mkdir /Library/FTPServer/FTPRoot/uploads
```

2. Set privileges for the folder to permit guest users to write to it:

```
$ chmod o + w /Library/FTPServer/FTPRoot/uploads
```

Changing the FTP User Environment

Use the Advanced pane of FTP service settings to change the user environment.

To change the FTP user environment:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Settings, then click Advanced.
5. From the "Authenticated users see" pop-up menu, choose the type of user environment you want to provide:
   - Use "FTP Root with Share Points" to set up the Users folder as a share point. Authenticated users log in to their home folders, if they're available. Authenticated and anonymous users can see other users' home folders.
   - Use "Home Folder with Share Points" to log authenticated FTP users in to their home folders. They have access to home folders, the FTP root, and FTP share points.
   - Use "Home Folder Only" to restrict authenticated FTP to user home folders.
6. Click Save.

Regardless of the user environment you choose, access to data is controlled by the access privileges that you or users assign to files and folders.

Anonymous users and authenticated users who don't have home folders (or whose home folders are not located in a share point they have access to) are always logged in at the root level of the FTP environment.

Changing the FTP Root Folder

Use the Advanced pane of FTP service settings to change the path to the FTP root folder.

To specify a different FTP root:

1. Select the folder you want to use.

   If the folder doesn't exist, create it and configure it as an FTP share point.
2. Open Server Admin and connect to the server.
3. Click the triangle at the left of the server.

   The list of services appears.
4. From the expanded Servers list, select FTP.
5. Click Settings, then click Advanced.
6. In the "FTP root" field, enter the path to the new folder or click the Choose button and select the folder.

From the command line:

You can also change the directory where FTP content is stored using the `serveradmin` command. By default, the directory is /Library/FTPServer/FTPRoot.

- To change where FTP content is stored:

```
$ sudo serveradmin settings ftp:ftpRoot = "value"
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Managing FTP Service

This section describes typical tasks you perform after you set up FTP service on your server. Initial setup information appears in "Setting Up FTP Service" on page 122.

Checking FTP Service Status

Use Server Admin to check the status of FTP service.

To view FTP service status:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select FTP.

4 To see whether the service is running, when it started, the number of authenticated and anonymous connections, and whether anonymous access is enabled, click Overview.

5 To review the event log, click Log.

6 To see a graph of connected users, click Graphs.

To choose the duration of time to graph data for, use the pop-up menu.

7 To see a list of connected users, click Connections.

The list includes the user name, type of connection, user IP address or domain name, and event activity.

From the command line:

- To see if the service is running:

```
$ sudo serveradmin status ftp
```

- To see complete status:

```
$ sudo serveradmin fullstatus ftp
```

- To view the FTP log:

```
$ tail log-file
```

By default, *log-file* is located in /Library/Logs/FTP.transfer.log. To see where the current transfer log is located, use the `serveradmin getLogPaths` command.

- To see a list of connected users:

```
$ ftpcount
```

or

```
$ sudo serveradmin command ftp:command = getConnectedUsers
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing the FTP Service Log

Use Server Admin to view the FTP log.

To view the FTP log:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select FTP.

4 Click Log.

To search for specific entries, use the Filter field in the upper right corner.

From the command line:
You can also view the FTP log using the `cat` or `tail` commands in Terminal.

- To view the FTP log:

```
$ tail log-file
```

By default, the *`log-file`* is located in the /Library/Logs/FTP.transfer.log. To see where the current transfer log is located, use the `serveradmin getLogPaths` command.

For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Viewing FTP Graphs

Use Server Admin to view FTP graphs.

To view FTP graphs:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. To see a graph of average connected user throughput over a period of time, click Graphs.

   To choose the duration of time to graph data for, use the pop-up menu.
5. To update the data in the graphs, click the Refresh button (below the Servers list).

Viewing FTP Connections

Use Server Admin to view clients that are connected to the server through FTP service.

To view FTP connections:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. To see a list of connected users, click Connections.

   The list includes user name, type of connection, user IP address or domain name, and event activity.
5. To update the list of connected users, click the Refresh button (below the Servers list).

From the command line:

- To view FTP connections:

```
$ ftpcount
```

or

```
$ sudo serveradmin command ftp:command = getConnectedUsers
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Stopping FTP Service

You stop FTP service using Server Admin.

To stop FTP service:

1. Open Server Admin and connect to the server.
2. Click the triangle at the left of the server.

   The list of services appears.
3. From the expanded Servers list, select FTP.
4. Click Stop FTP (below the Servers list).
5. Click Stop Now.

From the command line:

- To stop FTP service:

  ```
  $ sudo serveradmin stop ftp
  ```

  For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to Command-Line Administration*.

Solving Problems

8

Use this chapter to find solutions to common problems you might encounter while working with file services in Mac OS X Server.

Problems are listed in the following categories:

- Problems with share points
- Problems with AFP service
- Problems with SMB service
- Problems with NFS service
- Problems with FTP service

Problems with Share Points

This section describes potential problems with share points and ways to diagnose and resolve the problems.

If Users Can't Access Shared Optical Media

If users can't access shared optical media:

- Make sure the optical media is a share point.
- If you share multiple media, make sure that each has a unique name in the Sharing pane.

If Users Can't Access External Volumes Using Server Admin

Make sure the server is logged in.

If Users Can't Find a Shared Item

If users can't find a shared item:

- Check the access privileges for the item. The user must have Read access privileges to the share point where the item is located and to each folder in the path to the item.

- Server administrators don't see share points the same way a user does over AFP because administrators see everything on the server.

  To see share points from a user's perspective, select "Enable administrator to masquerade as any registered user" in the Access pane of the Settings pane of AFP service in Server Admin. You can also log in using a user's name and password.

- Although DNS is not required for file services, an incorrectly configured DNS could cause a file service to fail. For more information about DNS configuration, see *Network Services Administration.*

If Users Can't Open Their Home Folder

If users can't open their home folder:

- Make sure the share point used for home folders is set up as an automount for home folders in Server Admin.
- Make sure the share point is created in the same Open Directory domain as user accounts.
- Make sure the client computer is set to use the correct Open Directory domain using Directory Services in the Accounts pane of System Preferences.

If Users Can't Find a Volume or Folder to Use as a Share Point

If users can't find a volume or folder to use as a share point:

- Make sure the volume or folder name does not contain a slash ("/") character. The Share Points pane of Server Admin lists the volumes and folders on your server but it can't correctly display the names of volumes and folders that include the slash character.
- Make sure you're not using special characters in the name of the volume or folder.

If Users Can't See the Contents of a Share Point

If you set Write Only access privileges to a share point, users can't see its contents. Change the access privileges to Read Only or to Read & Write.

Problems with AFP Service

This section describes potential problems with AFP service and ways to diagnose and resolve them.

If Users Can't Find the AFP Server

If users can't find the AFP server:

- Make sure the network settings are correct on the user's computer and on the computer that is running AFP service. If you can't connect to other network resources from the user's computer, the network connection might not be working.

- Make sure the file server is running. Use the Ping pane in Network Utility to check whether the server at the specified IP address can receive packets from clients over the network.
- Check the name you assigned to the file server and make sure users are looking for the correct name.

If Users Can't Connect to the AFP Server

If users can't connect to the AFP server:

- Make sure the user has entered the correct user name and password. The user name is not case sensitive, but the password is.
- In the Accounts module of Workgroup Manager, verify that logging in is enabled for the user.
- See if the maximum number of client connections has been reached (in the AFP Service Overview). If it has, the user should try to connect later.
- Make sure the server that stores users and groups is running.
- Make sure IP Filter service is configured to enable access on port 548 if the user is trying to connect to the server from a remote location. For more on IP filtering, see *Network Services Administration*.

If Users Don't See the Login Greeting

If users can't see the login greeting, upgrade the software on their computer. AFP client computers must use AppleShare client software v3.7 or later.

Problems with SMB Service

This section describes potential SMB service problems and ways to diagnose and resolve them.

If Windows Users Can't See the Windows Server in Network Places

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

- Make sure the user's computer is configured for TCP/IP and has the correct Windows networking software installed.
- Make sure the user has guest access.
- Go to the DOS prompt on the client computer and enter `ping <IP address>`, where `<IP address>` is your server's address. If the ping fails, there is a TCP/IP problem.
- If the user is on a different subnet from the server, make sure you have a WINS server on your network.

  Note: If Windows computers are configured for networking and connected to the network, client users can connect to the file server even if they can't see the server icon in my Network Places.

If Users Can't Log In to the Windows (SMB) Server

If users can't log in to the Windows (SMB) Server, use the dirt command to make sure Password Server is configured correctly (if you are using Password Server to authenticate users). Also, verify the hash methods you enabled in Server Admin.

Problems with NFS Service

Following are general issues and recommendations to keep in mind when using NFS service:

- Not entering the full path to the NFS share point causes errors on the client side.
- If you export more than one NFS share point, you cannot have nested exports on a single volume, which means one exported directory cannot be the child of another exported directory on the same volume.
- To see available NFS mounts, use `showmount -e IP address` in Terminal, where *IP address* is the server's address.
- NFS server errors and warnings are logged to /var/log/system.log.
- `nfsd status` can be used to display the status of the NFS daemons.
- `nfsd checkexports` can be used to verify the current set of exports definitions.

For information about using NFS to host home folders, see *User Management*.

Problems with FTP Service

This section describes potential FTP service problems and ways to diagnose and resolve them.

If FTP Connections Are Refused

If FTP connections are refused:

- Verify that the user is entering the correct DNS name or IP address for the server.
- Make sure FTP service is on.
- Make sure the user has correct access privileges to the shared volume.
- See if the maximum number of connections has been reached. To do this, open Server Admin, select FTP in the Servers list, and click Overview. Note the number of connected users, click Settings, click General, and compare to the maximum user settings you have set.
- Verify that the user's computer is correctly configured for TCP/IP. If there doesn't appear to be a problem with TCP/IP settings, use the Ping pane in Network Utility to check network connections.
- See if there's a DNS problem by trying to connect using the IP address of the FTP server instead of its DNS name. If the connection works with the IP address, there might be a problem with the DNS server.

- Verify that the user is correctly entering his or her short name and password. User names and passwords with special characters or double-byte characters don't work. To find the user's short name, double-click the user's name in the Users & Groups list.
- See if there are problems with directory services, and make sure the directory services server is operating and connected to the network. For help with directory services, see *Open Directory Administration*.
- Verify that IP Filter service is configured to enable access to the correct ports. If clients still can't connect, see if the client is using FTP passive mode and turn it off. Passive mode causes the FTP server to open a connection to the client on a dynamically determined port, which could conflict with port filters set up in IP Filter service.
- Check the /Library/FTPServer/Messages/error.txt file for clues as to what the problem might be.

If Clients Can't Connect to the FTP Server

If users can't connect to the FTP server, see if the client is using FTP passive mode, and turn it off. Passive mode causes the FTP server to open a connection on a dynamically determined port to the client, which could conflict with port filters set up in IP Filter service.

If Anonymous FTP Users Can't Connect

If anonymous users can't connect to FTP service:

- Verify that anonymous access is turned on.
- See if the maximum number of anonymous user connections has been reached. To do this, open Server Admin and click FTP in the Servers list.

Command Line Parameters for File Services

Creating a Share Point

You can include the following parameters when creating a share point using the `sharing` command in Terminal.command

Parameter	Description
path	The full path to the folder you want to share.
customname	The name of the share point. If you don't specify the custom name, it's set to the name of the folder, the last name in `path`.
afpname	The share point name shown to and used by AFP clients. This name is not the same as the share point name.
ftpname	The share point name shown to and used by FTP clients.
smbname	The share point name shown to and used by SMB clients.
shareflags	A three-digit binary number indicating the protocols used to share the folder. The digits represent, from left to right, AFP, FTP, and SMB. `1`=shared, `0`=not shared.

Parameter	Description
guestflags	A group of flags indicating which protocols allow guest access. The flags are written as a three-digit binary number with the digits representing, from left to right, AFP, FTP, and SMB. `1`=guests allowed, `0`=guests not allowed.
inheritflags	A group of flags indicating whether new items in AFP or SMB share points inherit the ownership and access permissions of the parent folder. The flags are written as a two-digit binary number with the digits representing, from left to right, AFP and SMB. `1`=inherit, `0`=don't inherit.
creationmask	The SMB creation mask. Default=`0644`.
directorymask	The SMB folder mask. Default=`0755`.
oplockflag	A parameter that specifies whether opportunistic locking is allowed for an SMB share point. 1=enable oplocks, 0=disable oplocks.
strictlockingflag	A parameter that specifies whether strict locking is used on an SMB share point. `1`=enable strict locking, `0`=disable.

AFP Parameters

The following sections provide additional details about AFP parameters.

AFP Service Settings

You can configure the following AFP service settings using the `serveradmin` tool in Terminal.

Parameter (`afp:`)	Description
`activityLog`	Turn activity logging on or off. Default = `no`
`activityLogPath`	Location of the activity log file. Default = `/Library/Logs/AppleFileService/AppleFileServiceAccess.log`
`activityLogSize`	Rollover size (in kilobytes) for the activity log. Used only if `activityLogTime` isn't specified. Default = `1000`

Parameter (afp.)	Description
activityLogTime	Rollover time (in days) for the activity log. Default = 7
admin31GetsSp	Set to yes to force administrator users on Mac OS X to see share points instead of volumes. Default = yes
adminGetsSp	Set to yes to force administrator users on Mac OS 9 to see share points instead of volumes. Default = no
afpServerEncoding	Encoding used with Mac OS 9 clients. Default = 0
afpTCPPort	TCP port used by AFP on server. Default = 548
allowRootLogin	Allow user to log in as root. Default = no
attemptAdminAuth	Allow administrator user to masquerade as another user. Default = yes
authenticationMode	Authentication mode. Can be: • standard • kerberos • standard_and_kerberos Default = "standard_and_kerberos"
autoRestart	Enable AFP service to restart when abnormally terminated. Default = yes
clientSleepOnOff	Allow client computers to sleep. Default = yes
clientSleepTime	Time (in hours) that clients are allowed to sleep. Default = 24
createHomeDir	Create home folders. Default = yes

Parameter (afp.)	Description
enforce_unix_access	Allows UNIX computers access to AFP service. Default on server= yes Default on client= no
errorLogPath	Location of the error log. Default = /Library/Logs/AppleFileService/AppleFileServiceError.log
errorLogSize	Rollover size (in kilobytes) for the error log. Use only if errorLogTime isn't specified. Default = 1000
errorLogTime	Rollover time (in days) for the error log. Default = 0
guestAccess	Allow guest users access to the server. Default = yes
idleDisconnectFlag: adminUsers	Enforce idle disconnect for administrator users. Default = yes
idleDisconnectFlag: guestUsers	Enforce idle disconnect for guest users. Default = yes
idleDisconnectFlag: registeredUsers	Enforce idle disconnect for registered users. Default = yes
idleDisconnectFlag: usersWithOpenFiles	Enforce idle disconnect for users with open files. Default = yes
idleDisconnectMsg	Idle disconnect message. Default = ""
idleDisconnectOnOff	Enable idle disconnect. Default = no
idleDisconnectTime	Idle time (in minutes) allowed before disconnect. Default = 10
kerberosPrincipal	Kerberos server principal name. Default ="afpserver"

Parameter (afp.)	Description
lock_manager	Prevents simultaneous read/write access to shared files. Default = yes
loggingAttributes: logCreateDir	Record folder creations in the activity log. Default = yes
loggingAttributes: logCreateFile	Record file creations in the activity log. Default = yes
loggingAttributes: logDelete	Record file deletions in the activity log. Default = yes
loggingAttributes: logLogin	Record user logins in the activity log. Default = yes
loggingAttributes: logLogout	Log user logouts in the activity log. Default = yes
loggingAttributes: logOpenFork	Log file opens in the activity log. Default = yes
loginGreeting	Login greeting message. Default = ""
loginGreetingTime	Last time the login greeting was set or updated.
maxConnections	Maximum simultaneous user sessions allowed by the server. Default = -1 (unlimited)
maxGuests	Maximum simultaneous guest users allowed. Default = -1 (unlimited)
maxThreads	Maximum AFP threads. (Must be specified at startup.) Default = 40
noNetworkUsers	Indication to client that all users are users on the server. Default = no

Parameter (afp.)	Description
recon1SrvrKeyTTLHrs	Time-to-live (in hours) for the server key used to generate reconnect tokens. Default = 168
recon1TokenTTLMins	Time-to-live (in minutes) for a reconnect token. Default = 10080
reconnectFlag	Allow reconnect options. Can be set to: • none • all • no_admin_kills Default = "all"
reconnectTTLInMin	Time-to-live (in minutes) for a disconnected session waiting reconnection. Default = 1440
registerAppleTalk	Advertise the server using AppleTalk NBP. Default = yes
registerNSL	Advertise the server using Bonjour. Default = yes
sendGreetingOnce	Send the login greeting only once. Default = no
shutdownThreshold	Don't modify. Internal use only.
specialAdminPrivs	Grant administrator users root user read/write privileges. Default = no
TCPQuantum	TCP message quantum. Default = 262144
tcpWindowSize	The amount of data that can be sent on a connection before receiver acknowledgment. Default = 64
tickleTime	Frequency of tickles sent to client. Default = 30
updateHomeDirQuota	Enforce quotas on the user's volume. Default = yes
useAppleTalk	Don't modify. Internal use only.

AFP serveradmin Commands

To manage AFP service, use the following commands with serveradmin.

Command (afp:command=)	Description
cancelDisconnect	Cancel a pending user disconnect.
disconnectUsers	Disconnect AFP users.
getConnectedUsers	List settings for connected users.
getHistory	View a periodic record of file data throughput or number of user connections.
getLogPaths	Display the locations of the AFP service activity and error logs.
sendMessage	Send a text message to connected AFP users.
syncSharePoints	Update share point information after changing settings.
writeSettings	Equivalent to the standard *serveradmin settings* command, but also returns a setting indicating whether the service must be restarted.

FTP Parameters

The following sections provide additional details about FTP parameters.

FTP Service Settings

You can configure the following FTP service settings using the `serveradmin` tool in Terminal.

Parameter (ftp:)	Description
administratorEmailAddress	Sets the administrator mail address. Default = "user@hostname"
anonymous-root	Sets the anonymous root directory. Default = "/Library/FTPServer/FTPRoot"
anonymousAccessPermitted	Allows anonymous access to FTP if you change the default setting to yes. Default = no

Parameter (ftp.)	Description
authLevel	Sets the authentication method. "KERBEROS" and "ANY METHOD" are the other possible values. Default = "STANDARD"
bannerMessage	Displays a banner message that appears when you are prompted to log in to FTP. Customize to your own preferences. Default ="----------This is the "Banner" message for the Mac OS X Server's FTP server process. FTP clients will receive this message immediately before being prompted for a name and password. PLEASE NOTE: Some FTP clients may exhibit problems if you make this file too long. ----------"
chrootType	Default = "STANDARD"
enableMacBinAndDmgAutoConversion	Default = yes
ftpRoot	The directory where the FTP content is stored. Default = "/Library/FTPServer/FTPRoot"
logCommands:anonymous	Default = no
logCommands:guest	Default = no
logCommands:real	Default = no
loginFailuresPermitted	Default = 3
logSecurity:anonymous	Default = no
logSecurity:guest	Default = no
logSecurity:real	Default = no
logToSyslog	Default = no
logTransfers:anonymous:inbound	Default = yes
logTransfers:anonymous:outbound	Default = yes
logTransfers:guest:inbound	Default = no
logTransfers:guest:outbound	Default = no
logTransfers:real:inbound	Default = yes
logTransfers:real:outbound	Default = yes

Parameter (ftp.)	Description
maxAnonymousUsers	Default = 50
maxRealUsers	Default = 50
showBannerMessage	Default = yes
showWelcomeMessage	Default = yes
welcomeMessage	Displays a welcome message that appears after you log in to FTP. Customize to your own preferences. Default = "---------- ----------This is the "Welcome" message for the Mac OS X Server's FTP server process. FTP clients will receive this message right after a successful log in. ---------- ---"

FTP serveradmin Commands

To manage FTP service, use the following commands with serveradmin.

Command (ftp:command=)	Description
getConnectedUsers	View connected users.
getLogPaths	Show location of the FTP transfer log file.
writeSettings	Equivalent to the standard serveradmin settings command, but also returns a setting indicating whether the service must be restarted.

SMB Parameters

The following sections provide additional details about SMB parameters.

SMB Service Settings

You can configure the following SMB service settings using the serveradmin tool in Terminal.

Parameter (smb.)	Description
adminCommands:homes	Whether home folders are mounted when Windows users log in so you don't need to set up share points for each user. Can be set to: yes | no This corresponds to the "Enable virtual share points" checkbox in the Advanced pane of Windows service settings in Server Admin.
adminCommands:serverRole	The authentication role played by the server. Can be set to: • standalone • domainmember • primarydomaincontroller • backupdomaincontroller This corresponds to the Role pop-up menu in the General pane of Windows service settings in Server Admin.
domain master	Whether the server is providing Windows domain master browser service. Can be set to: yes | no This corresponds to the Domain Master Browser checkbox in the Advanced pane of Windows service settings in Server Admin.

Parameter (smb.)	Description
dos charset	The code page being used. Can be set to: • 437 (Latin US) • 737 (Greek) • 775 (Baltic) • 850 (Latin1) • 852 (Latin2) • 861 (Icelandic) • 866 (Cyrillic) • 932 (Japanese SJIS) • 936 (Simplified Chinese) • 949 (Korean Hangul) • 950 (Traditional Chinese) • 1251 (Windows Cyrillic) This corresponds to the Code Page pop-up menu on the Advanced pane of Windows service settings in Server Admin.
local master	Whether the server is providing Windows workgroup master browser service. Can be set to: yes | no This corresponds to the Workgroup Master Browser checkbox in the Advanced pane of Windows service settings in Server Admin.
log level	The amount of detail written to the service logs. Can be set to: • 0 (Low: errors and warnings only) • 1 (Medium: service start and stop, authentication failures, browser name registrations, and errors and warnings) • 2 (High: service start and stop, authentication failures, browser name registration events, log file access, and errors and warnings) This corresponds to the Log Detail pop-up menu in the Logging pane of Windows service settings in Server Admin.

Parameter (`smb.`)	Description
`map to guest`	Whether guest access is allowed. Can be set to: • `"Never"` (No guest access) • `"Bad User"` (Allow guest access) This corresponds to the "Allow Guest access" checkbox in the Access pane of Window service settings in Server Admin.
`max smbd processes`	The maximum allowed number of smbd server processes. Each connection uses its own smbd process, so this is the same as specifying the maximum number of SMB connections. `0` means unlimited. This corresponds to the "maximum" client connections field in the Access pane of the Windows service settings in Server Admin.
`netbios name`	The server's NetBIOS name. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the "Computer Name" field in the General pane of the Windows service settings in Server Admin.
`server string`	Text that helps identify the server in the network browsers of client computers. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the "Description field" in the General pane of the Windows service settings in Server Admin.
`wins support`	Whether the server provides WINS support. Can be set to: `yes | no` This corresponds to the WINS Registration "Off" and "Enable WINS" server options in the Advanced pane of the Windows service settings in Server Admin.
`wins server`	The name of the WINS server used by the server. This corresponds to the WINS Registration "Register with WINS server" option and field in the Advanced pane of the Windows service settings in Server Admin.
`workgroup`	The server's workgroup. Can be set to a maximum of 15 bytes of UTF-8 characters. This corresponds to the "Workgroup" field in the General pane of the Windows service settings in Server Admin.

SMB serveradmin Commands

To manage SMB service, use the following commands with `serveradmin`.

Command (`smb:command=`)	Description
`disconnectUsers`	Disconnect SMB users.
`getConnectedUsers`	List users connected to an SMB service.
`getHistory`	List connection statistics.
`getLogPaths`	Show location of service log files.
`syncPrefs`	Update the service to recognize changes in share points.
`writeSettings`	Equivalent to the standard `serveradmin settings` command, but also returns a setting indicating whether the service must be restarted.

Index

D

E

F

G

H

I

K

V

W