Mac OS X Server

File Services Administration
For Version 10.4 or Later

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

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

019-0161/03-24-2005

Contents

About This Guide

Learn what's new for Mac OS X Server File Services Administration.

Mac OS X Server version 10.4 offers reliable, high-performance file services using native protocols for Mac, Windows, and Linux workgroups. The server is designed to fit seamlessly into virtually any environment including mixed enterprise networks. Mac OS X Server v10.4 delivers expanded function of current features and introduces additional features to enhance support for heterogeneous networks, maximize user productivity, and make file services more secure and easier to manage.

What's New in Version 10.4

- Access Control Lists (ACLs)—ACLs go beyond the limitations of traditional Portable Operating System Interface (POSIX) file permissions to give you greater flexibility over assigning access permissions to files, folders and network services. ACLs in Mac OS X Server are compatible with those in Windows servers.
- NFS resharing—You can now use Workgroup Manager to reshare NFS volumes using AFP, which, unlike NFS, provides service discovery and secure authentication.
- Unified locking—Mac OS X Server unifies file locking across AFP and SMB/CIFS protocols. This feature lets users working on multiple platforms simultaneously share files without worrying about file corruption.

What's in This Guide

This guide includes the following chapters:

- Chapter 1, "Overview of File Services," provides an overview of Mac OS X Server file services, explains standard permissions and ACLs, and discusses related security issues.
- Chapter 2, "Setting Up Share Points," describes how to share specific volumes and directories via the Apple Filing Protocol (AFP), Server Message Block (SMB)/Common Internet File System (CFIS), File Transfer Protocol (FTP), and Network File System (NFS) protocols. It also describes how to set standard and ACL permissions.

- Chapter 3, "AFP Service," describes how to set up and manage AFP service in Mac OS X Server.
- Chapter 4, "NFS Service," describes how to set up and manage the NFS service in Mac OS X Server.
- Chapter 5, "FTP Service," describes how to set up and manage FTP service in Mac OS X Server.
- Chapter 6, "Solving Problems," lists possible solutions to common problems you might encounter while working with the file services in Mac OS X Server.
- The Glossary provides brief definitions of terms used in this guide.

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

Using Onscreen Help

You can view instructions and other useful information from this and other documents in the server suite by using onscreen help.

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

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

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

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

The Mac OS X Server Suite

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

www.apple.com/server/documentation/

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

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

Getting Documentation Updates

Periodically, Apple posts new onscreen help topics, revised guides, and additional solution papers. The new help topics include updates to the latest guides.

- To view new onscreen help topics, make sure your server or administrator computer is connected to the Internet and click the Late-Breaking News link on the main Mac OS X Server help page.
- To download the latest guides and solution papers in PDF format, go to the Mac OS X Server documentation webpage: www.apple.com/server/documentation.

Getting Additional Information

For more information, consult these resources:

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

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

AppleCare Service & Support—access to hundreds of articles from Apple's support organization.
www.apple.com/support/

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

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

Apple mailing list directory—subscribe to mailing lists so you can communicate with other administrators using email.
discussions.info.apple.com/

Apple Filing Protocol (AFP) website—manual describing AFP.
developer.apple.com/documentation/Networking/Conceptual/AFP/

Samba website—information about Samba, the open source software on which the Windows services in Mac OS X Server are based.
www.samba.org/

Common Internet File System (CIFS) website—detailed description of how CIFS works.
www.ubiqx.org/cifs/

File Transfer Protocol (FTP) website—home of the FTP Request for Comments (RFC) document.
www.faqs.org/rfcs/rfc959.html

File Transfer Protocol (TFTP) website—home of the TFTP RFC document.
asg.web.cmu.edu/rfc/rfc1350.html

Note: RFC documents provide an overview of a protocol or service that can be helpful for novice administrators, as well as more detailed technical information for experts. You can search for RFC documents at www.faqs.org/rfcs.

Overview of File Services

1

This chapter provides an overview of Mac OS X Server file services, explains standard permissions and Access Control Lists (ACLs), and discusses related security issues.

You can configure Mac OS X Server file services to allow clients to access shared files, applications, and other resources over a network.

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

Note: This guide describes how to set up AFP, FTP, and NFS services. For information about setting up Windows service, refer to the Windows services administration guide.

Multiple Network Interface Support

AFP, SMB/CIFS, FTP, and NFS file services are available over all network interfaces in Mac OS X Server. You can't configure file services separately for each interface.

Setting Up File Services

You use the following applications to set up and manage file services:

- Server Admin: Use it to configure individual file services for each protocol.
- Workgroup Manager: Use it to create share points and set access privileges.

You can also perform most setup and management tasks in Terminal. For more information, see the file services chapter of the command-line administration guide.

Permissions in the Mac OS X Environment—Background

If you're new to Mac OS X and are not familiar with UNIX, it's important to know that there are some differences in the way ownership and permissions are handled compared to Mac OS 9.

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."

Files and folders are, by default, owned by the user who creates them. After they're created, items keep their privileges (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 client users if they are created in a folder for which the users don't have privileges. When setting up share points, make sure that items allow appropriate access privileges for the users with whom you want to share them.

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 Portable Operating System Interface (POSIX) permissions let you control access to files and folders based on three categories of users: Owner, Group, and Everyone. While 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 allows 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.

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

Standard Permissions

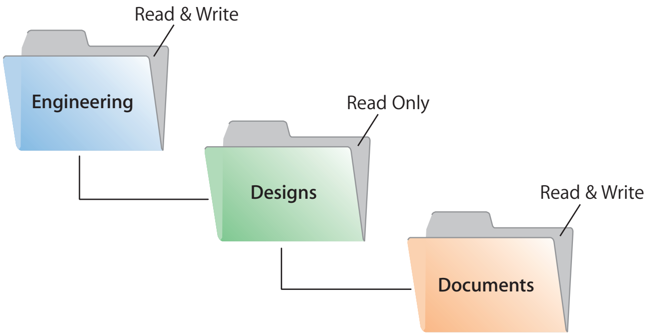
There are four types of standard POSIX access permissions that you can assign to a share point, folder, or file: Read & Write, Read Only, Write Only, and None. The table below shows how these permissions affect user access to different types of shared items (files, folders, and share points).

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

Note: QuickTime Streaming Server and WebDAV have separate permissions settings. For information about QTSS, refer to the QTSS online help and the QuickTime website (www.apple.com/quicktime/products/qtss/). You'll find information about Web permissions in the Web technologies administration guide.

Explicit Permissions

Share points and the shared items they contain (including both folders and files) have separate permissions. If you move an item to a different folder, it retains its own permissions and doesn't automatically 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/CIFS share point so that new files and folders inherit the permissions of their parent folder. See "Changing Apple File Settings for a Share Point" on page 35, or "Changing Windows (SMB/CIFS) Settings for a Share Point" on page 36.

The User Categories Owner, Group, and Everyone

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

- Owner—A user who creates a new item (file or folder) on the file server is its owner and automatically has Read & Write 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 (allow a group or everyone to use the item). The administrator can also transfer ownership of the shared item to another user.

  Note: When you copy an item to a drop box on an Apple file server, ownership of the item doesn't change, but 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 into group accounts. Only one group can be assigned access permissions to a shared item. For more information on creating groups, see the user management guide.
- Everyone—Everyone is any user who can log in to the file server: registered users and guests.

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 Everyone permissions.
- Owner permissions override Group permissions.

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

Client Users and Permissions

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

Standard Permission Propagation

Workgroup Manager provides a command that lets you specify which standard permissions to propagate. For example, you can use this command to propagate only the permission for Everyone to all descendants of a folder, and leave the permissions for Owner and Group unchanged. For more information on how to use this command, see "Propagating Permissions" on page 46.

ACLs

When standard POSIX permissions are not enough, you can 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 let you set file and folder access permissions to multiple users and groups, in addition to the 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 directory that allows 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 creation of only folders and not files.

Apple's ACL model supports 13 permissions for controlling access to files and folders:

- Administration
  - *Change Permissions:* User can change standard permissions
  - *Take Ownership*: User can change the file's or folder's ownership to him or herself
- Read
  - *Read Attributes:* User can view the file's or folder's attributes (for example, name, date, and size)
  - *Read Extended Attributes:* User can view the file's or folder's attributes added by third-party developers
  - *List Folder Contents (Read Data):* User can list folder contents and read files
  - *Traverse Folder (Execute File):* User can open subfolders and execute a program
  - *Read Permissions:* User can view the file's or folder's standard permissions using the Get Info or Terminal commands
- Write
  - *Write Attributes:* User can change the file's or folder's standard attributes
  - *Write Extended Attributes:* User can change the file's or folder's other attributes
  - *Create Files (Write Data):* User can create files and modify files
  - *Create Folder (Append Data):* User can create subfolders and add new data to files
  - *Delete:* User can delete file or folder
  - *Delete Subfolders and Files:* 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 all descendants (see "Understanding Inheritance" on page 21 to learn how this option works with the previous two)

The ACL Use Model

The ACL use model is centered around access control at the folder level, with ACLs applied to files as the result of inheritance.

Folder-level control defines which users have access to the contents of a folder, and inheritance defines how a defined set of permissions and rules pass from the container to the objects within it.

Without use of this model, administration of access control would quickly become a nightmare: you would have to create and manage ACLs on thousands or millions of files. In addition, controlling access to files through inheritance frees applications from having to maintain extended attributes or explicit ACEs when saving a file because the system automatically applies inherited ACEs to files (see "Explicit and Inherited ACEs" on page 21 for information about explicit ACEs).

ACLs and Standard Permissions

You can set ACL permissions for files and folders in addition to standard permissions. See "Rules of Precedence" on page 24 for more information on how Mac OS X Server uses ACL and standard permissions to determine what users can and cannot do to a file or folder.

ACL Management

In Mac OS X Server, you can create and manage ACLs in the Access pane of the Sharing pane of Workgroup Manager, but you can't do so in the Get Info window in Finder. The Get Info window, however, will display the logged-in user's effective permissions. See "Setting ACL Permissions" on page 34, and "Managing Share Point Access Privileges" on page 43 for instructions on how to set and manage ACLs.

In addition to Workgroup Manager, you can set and view ACL permissions on both Mac OS X and Mac OS X Server using the command-line tools `ls` and `chmod`. See the corresponding man pages and the command-line administration guide for more information.

Using Workgroup Manager, you can define ACLs for share points and folders. As for files, they get their ACLs through inheritance, as stated earlier.

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

An access control entry (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/Group
- Permission Type
- Permission
- Inherited

User/Group

An ACE stores a universally unique ID for a group or user, which permits unambiguous resolution of identity.

Permission Type

An ACE supports two permission types:

- Allow—If you choose Allow, you grant permissions by selecting them in Workgroup Manager.
- Deny—If you choose Deny, you withhold permissions by deselecting them in Workgroup Manager.

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.

Explicit and Inherited ACEs

Workgroup Manager supports two types of ACEs: Explicit ACEs and inherited ACEs. Explicit ACEs are the ones you create in an ACL (see "Adding ACEs to ACLs" on page 44). Inherited ACEs, however, are ACEs you have created for a parent folder, which have been inherited by a descendant file or folder.

To help you tell the difference between explicit and inherited ACEs, Workgroup Manager displays inherited ACEs as dimmed entries.

Note: Inherited ACEs cannot be edited unless you make them explicit. Workgroup Manager allows you to convert an inherited ACE to an explicit ACE. See "Making a Folder's Inherited ACE Entries Explicit" on page 46 for more information.

Understanding Inheritance

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

The Apple ACL Inheritance Model

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

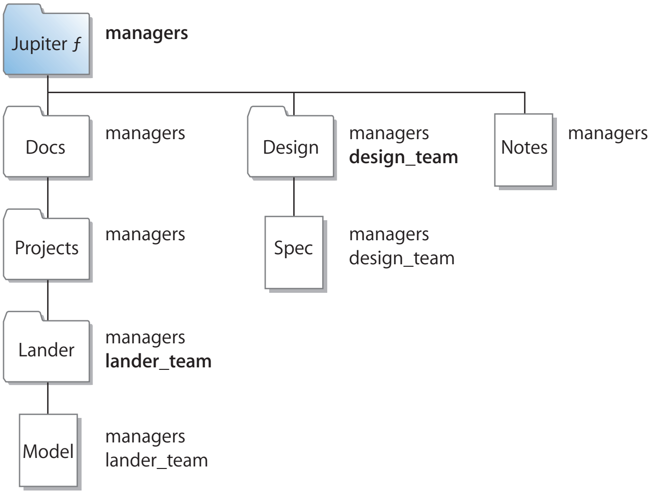
Inheritance option	Description
Apply to this folder	Apply (Administration, Read, and Write) permissions to this folder
Apply to child folders	Apply permissions to subfolders
Apply to child files	Apply permissions to the files in this folder
Apply to all descendants	Apply permissions to all descendants[1]

[1] 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. See "ACL Inheritance Combinations" on page 23 for more information.

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

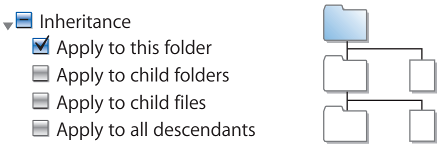
- By the kernel at file or folder creation time—When you create a file or folder, the kernel determines what permissions the file or folder inherits from its parent folder.
- By administrative tools after creating an explicit ACE—For example, after you set ACL permissions for a folder, Workgroup Manager propagates the new permissions to the applicable descendants.

The figure below shows how Workgroup Manager propagates two ACEs (managers and design_team) after ACE creation. Bold text represents an explicit ACE and regular text an inherited ACE.

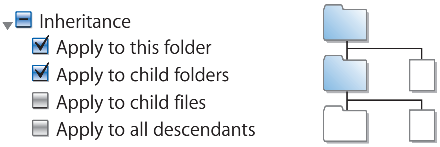


ACL Inheritance Combinations

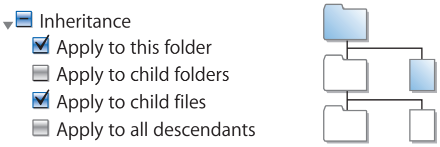
When you set inheritance options for an ACE in Workgroup Manager, you can choose from 12 unique inheritance combinations for propagating ACL permissions.



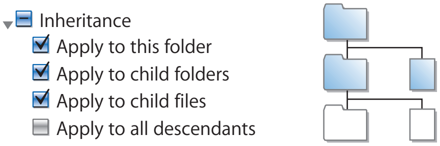
▾ ⊟ Inheritance
- ☑ Apply to this folder
- □ Apply to child folders
- □ Apply to child files
- □ Apply to all descendants



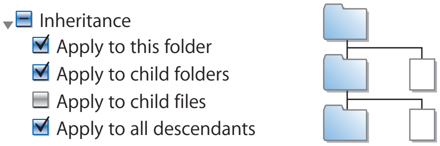
▾ ⊟ Inheritance
- ☑ Apply to this folder
- ☑ Apply to child folders
- □ Apply to child files
- □ Apply to all descendants



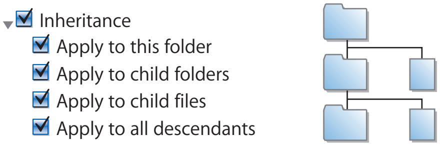
▾ ⊟ Inheritance
- ☑ Apply to this folder
- □ Apply to child folders
- ☑ Apply to child files
- □ Apply to all descendants



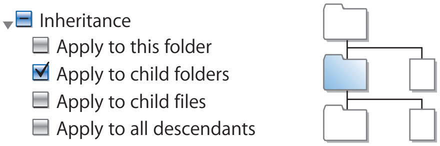
▾ ⊟ Inheritance
- ☑ Apply to this folder
- ☑ Apply to child folders
- ☑ Apply to child files
- □ Apply to all descendants



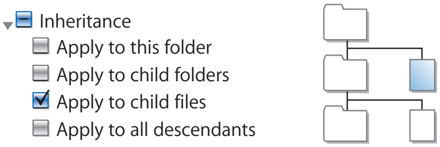
▾ ⊟ Inheritance
- ☑ Apply to this folder
- ☑ Apply to child folders
- □ Apply to child files
- ☑ Apply to all descendants



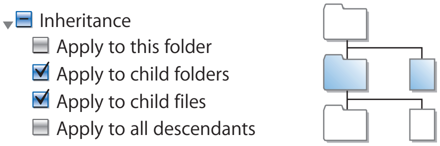
▾ ☑ Inheritance
- ☑ Apply to this folder
- ☑ Apply to child folders
- ☑ Apply to child files
- ☑ Apply to all descendants



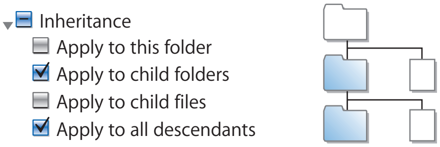
▾ ⊟ Inheritance
- □ Apply to this folder
- ☑ Apply to child folders
- □ Apply to child files
- □ Apply to all descendants



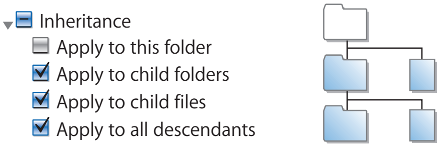
▾ ⊟ Inheritance
- □ Apply to this folder
- □ Apply to child folders
- ☑ Apply to child files
- □ Apply to all descendants



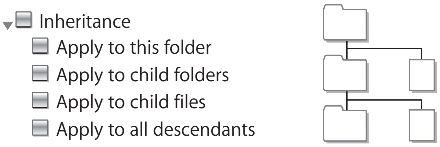
▾ ⊟ Inheritance
- □ Apply to this folder
- ☑ Apply to child folders
- ☑ Apply to child files
- □ Apply to all descendants



▾ ⊟ Inheritance
- □ Apply to this folder
- ☑ Apply to child folders
- □ Apply to child files
- ☑ Apply to all descendants



▾ ⊟ Inheritance
- □ Apply to this folder
- ☑ Apply to child folders
- ☑ Apply to child files
- ☑ Apply to all descendants

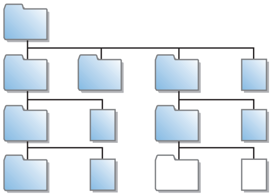


▾ □ Inheritance
- □ Apply to this folder
- □ Apply to child folders
- □ Apply to child files
- □ Apply to all descendants

ACL Permission Propagation

Workgroup Manager provides a command that lets you force the propagation of ACLs. While this is done automatically by Workgroup Manager, there are cases when this command comes in handy:

- You can use this command 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 all descendants. Then, you select the root folder of the subtree and use the command to remove the ACLs from all descendants of that subtree. In the example below, the items in white had their ACLs removed by the propagation command.



- You can use this command to reapply inheritance in cases where you removed a folder's ACLs and decided to reapply them.
- You can use this command to clear all ACLs at once instead of having to go through a folder hierarchy and manually remove ACEs.

For more information on how to use this command, see "Propagating Permissions" on page 46.

Rules of Precedence

When you add ACEs to an ACL, order is important. Mac OS X Server uses the following rules to control access to files and folders:

- If a file or folder has no ACEs defined for it, Mac OS X Server applies the standard POSIX permissions.
- If a file or folder has one or more 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. After evaluating the ACEs, Mac OS X Server evaluates the standard POSIX permissions defined on the file or folder. Then, based on the evaluation of ACL and standard POSIX permissions, Mac OS X Server determines what type of access a user has to a shared file or folder.

Deny Permissions Override Other Permissions

When you add ACEs, Workgroup Manager places Deny permissions above Allow permissions because they have precedence over allow permissions. When evaluating permissions, whenever Mac OS X Server finds a Deny permission, it ignores all other permissions the user has in the same ACL and applies the Deny permission.

For example, if you add an ACE for the user Mai and allow her reading permissions and then add another ACE for a group in which Mai is member and deny the group reading permissions, Workgroup Manager will reorder the permissions so that the Deny permission is above the allow permission. The result is that Mac OS X Server applies the Deny permission for Mai and ignores the Allow permission for Mai's group.

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.

Tips and Advice

Mac OS X Server combines both traditional POSIX permissions with ACLs. This combination provides you with great flexibility and a fine level of granularity in controlling access to files and folders. But at the same time, these benefits have side effects. If you're not careful in how you assign privileges, things will quickly get out of hand and become very confusing. It'll be very hard for you to keep track of how permissions are assigned.

Note: With 17 permissions, you can choose from a staggering 98,304 combinations. Add to that a complex folder hierarchy, many users and groups, and many exceptions, and you have a recipe for complete confusion if not disaster.

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 and assign them only to individual users when there is an exception. For example, you can assign all teachers in a school district Read and Write permissions to a certain share point, but deny Miss Buxton, a temporary teacher, permission to read a certain 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 having to reassign permissions.

Gradually Add Permissions

Assign only necessary permissions and gradually add permissions 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 appropriate in the folder hierarchy, you can give the group additional reading and writing permissions.

Use the Deny Rule Only When You Need To

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. In addition, you might want to keep a record of these Deny permissions so that 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 that users have the appropriate access to important resources. This is especially important after modifying ACLs. Sometimes, you might inadvertently give someone more or fewer permissions than they need. The inspector helps you detect these cases. For more information about this inspector, see "Determining User or Group Permissions to a File or Folder" on page 47.

Protect Applications From Being Modified

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

Keep It Simple

Sometimes, you can unnecessarily complicate file access management if you're not careful. So just keep it simple. If standard POSIX permissions do the job, then use those. But if you need to use ACLs, avoid customizing permissions unless you have to.

Also, use simple folder hierarchies as much as possible. A little bit of strategic planning can help you create effective and manageable shared hierarchies.

File Services Access Control

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

Using SACLs allows you to add another layer of access control on top of standard and ACL permissions. Only users and groups listed in a SACL have access to its corresponding service. For example, if you want to prevent users from accessing a server's AFP share points, including home directories, just remove the users from the AFP service's SACL. See "Setting SACL Permissions" on page 51 for instructions on how to restrict access to file services using SACLs.

Customizing the Mac OS X Network Globe

The Network globe you find at the top level of a Mac OS X Finder window contains shared network resources. You can customize the contents of the Network globe to suit your clients by setting up automatically mounting share points. You can provide automatic access to system resources such as fonts and preferences by automatically mounting share points containing them in specific directory locations.

Share Points in the Network Globe

The Network globe on Mac OS X clients represents the /Network directory. By default, the Network globe contains at least these folders:

- Applications
- Library
- Servers

You can mount share points into any of these folders. See "Automatically Mounting Share Points for Clients" on page 40 for instructions.

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

Adding System Resources to the Network Library Folder

The Library folder in the Network globe is included in the system search path. This gives you the ability to make available, over the network, any type of system resource usually found in the local Library folder. 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 wish to have a specific set of fonts available to each user in a given Open Directory domain. You would create a share point containing the desired fonts and then set the share point to mount automatically as a shared library in /Network/Library/Fonts on client machines. See "Automatically Mounting Share Points for Clients" on page 40 for more information.

Security Considerations

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

Restricting Access to File Services

As stated in "File Services Access Control" on page 26, you can use Service Access Control Lists (SACLs) to restrict access to AFP, FTP, and Windows 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 service), could potentially expose your data to anyone on the Internet.

Restricting Access to NFS Share Points

NFS share points don't have the same level of security as AFP and SMB/CIFS, which require user authentication (typing a user name and password) to gain access to a share point's contents. If you have NFS clients, you may want to set up a share point to be used only by NFS users.

Note: NFS doesn't support ACLs.

Restricting Guest Access

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

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, you can take these precautions using the Sharing module of Workgroup Manager:

- Depending on what controls you want to place on guest access to a share point, you might consider one of 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 within it.
  - Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder.
- 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

2

This chapter describes how to share specific volumes and directories via the AFP, SMB/CFIS, FTP, and NFS protocols. It also shows how to set standard and ACL permissions.

You use the Sharing module of Workgroup Manager to share information with clients of the Mac OS X Server and control access to shared information by assigning access privileges.

To share individual folders or entire volumes that reside on the server, you 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 privileges to access share points see them as volumes mounted on their desktops or in their Finder windows.

Share Points and the Mac OS X Network Globe

If your Mac OS X operating system is configured to connect to LDAP directory domains and set up per specific data mapping, you can control the access and availability of various network services by using the Workgroup Manager application to:

- Identify share points and shared domains that you want to mount automatically in a user's /Network directory (the Network globe in Finder windows).
- Define user records and group records and configure their settings.
- Define lists of computers that have the same preference settings and are available to the same users and groups.

Automounting

You can configure client computers to automatically mount share points, which can be static or dynamic.

Static share points are mounted on a client computer during startup and its contents are immediately available when selected. You can assign statically mounted share points specific directories within the /Network directory (the Network globe).

Dynamic share points always reside inside the Network globe in /Network/Servers/server_name and don't mount until a client selects them.

The benefit of static share points is that they can be assigned to specific directories as mentioned above, while dynamic share points use fewer server resources when they're not in use.

Share Points and Network Home Directories

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

A home directory share point is mounted by the user's account at the time of login and provides the user the same environment to store files as if the directories were on the local computer. The benefit of Network Home Directories (NHD) is that they can be accessed by any client computer that can log in to a specific server providing NHD services for that user.

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 directories
- Disk quotas

Client Privileges

Before you set up a share point, you need to 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 1 (see "Kinds of Permissions" on page 16).

File Sharing Protocols

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

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

Note: Unified locking across AFP, SMB/CIFS, and NFS protocols lets users working on multiple platforms simultaneously share files without worrying about file corruption.

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 can be used on either file protocol. In a case such as this, you can create a single share point that supports both platforms.

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

If most of your clients are UNIX users and just a few are Mac OS clients, you may want to share items using only NFS to keep your setup simple. Keep in mind, however, that NFS doesn't provide many AFP features that Mac OS users are accustomed to, such as performance optimization or quick file searching.

Also, if you share applications or documents that are exclusively for Windows users, you can set up an SMB/CIFS share point to be used only by them. This provides a single point of access for your Windows users and lets them take advantage of both opportunistic and strict file locking. For more information about file locking, see the chapter on administering Windows users, groups, computers, and share points in the Windows services administration guide.

Note: If you enable both AFP and Windows services on your server, Mac OS clients can connect to the server over AFP or SMB/CIFS. Windows users will need to use third-party AFP client software to connect to your server over AFP.

Shared Information Organization

Once you have created share points, users will start to 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. If you can, organize shared information before you set up the share points. This is especially important if you're setting up network home directories.

Security

Review the issues discussed in "Security Considerations" on page 27.

Network Home Directories

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

- The share point /Users is set up by default to be used for storing home directories when you install Mac OS X Server. You can use this preconfigured share point for user home directories or create a new one on any local volume.
- The Network Mount settings for the share point should indicate that it's used for user home directories.

- The share point should be in the same Open Directory domain where the user accounts are defined.
- To provide service to all types of clients, the complete pathname of an AFP or NFS network home directory must not contain spaces and must not exceed 89 characters. For more information, see the Apple Knowledge Base article107695 at docs.info.apple.com/article.html?artnum=107695.

Important: You should store home directories in AFP share points, because AFP provides authentication-level access security, which a service such as NFS does not provide. With AFP, a user must log in with a valid name and password to access files.

Disk Quotas

You can limit the disk space a user's home directory can occupy by setting a quota on the Home pane of the user's account settings in Workgroup Manager.

To set space quotas for other share points, you must use the command line. See the file services chapter of the command-line administration guide.

Setup Overview

You use the Sharing module of Workgroup Manager to create share points and set privileges for them.

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

Step 1: Read "Before You Begin"

Read "Before Setting Up a Share Point" on page 30 for issues you should consider before sharing information on your network.

Step 2: Locate or create the information you want to share

Decide which volumes, partitions, or folders you want to share. You may want to move folders and files to different locations before setting up the share point. You may want to partition a disk into volumes so you can give each volume different access privileges or create folders that will have different levels of access. See "Shared Information Organization" on page 31.

Step 3: Set up share points and set privileges

When you designate an item to be a share point, you set its privileges at the same time. You create share points and set privileges in the Sharing module of Workgroup Manager. See "Setting Up a Share Point" on page 33.

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 Apple File Protocol with your share point, you must turn on AFP service. You can share an item using more than one protocol. See Chapter 3, "AFP Service," on page 53; Windows Services administration guide; Chapter 4, "NFS Service," on page 69; or Chapter 5, "FTP Service," on page 75.

Setting Up a Share Point

This section describes:

- How to create share points
- How to set share point access privileges
- How to share using specific protocols (AFP, SMB/CIFS, FTP, or NFS)
- How to automatically mount share points on clients' desktops

See "Managing Share Points" on page 41 for additional tasks that you might perform after you have set up sharing on your server.

Creating a Share Point

You use the Sharing module of Workgroup Manager 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 Workgroup Manager and click Sharing.

2. Click All and select the item you want to share.

3. Click General.

4. Select "Share this item and its contents."

5. Click Save.

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

To change protocol settings, stop sharing via a particular protocol, or export the share point using NFS, click Protocol and choose the protocol from the pop-up menu. Settings specific to each protocol are described in the following sections.

From the Command Line

You can also set up a share point using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Setting Privileges

Mac OS X Server provides two methods of access control to files and folders:

- Standard POSIX permissions
- Access Control Lists (ACLs)

These methods are described in the following sections.

Setting Standard Permissions

When you don't require the flexibility and granularity that access control lists (ACLs) provide, or in cases where ACLs are not supported, you can use the 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 Workgroup Manager and click Sharing.
2. Click Share Points and select the share point.
3. Click Access.
4. To set the owner or group of the shared item, type names or drag names from the Users & Groups drawer.

   To open the drawer, click Users & Groups. If you don't see a recently created user or group, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences and change the value of the "Auto-refresh Sharing every" field.
5. Use the pop-up menus next to the fields to change the permissions for the Owner, Group, and Everyone.

   Everyone is any user who is not the owner and does not belong to the group but can log in to the file server: other registered users and guests.
6. Click Save.

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

Setting ACL Permissions

To configure access control list (ACL) permissions for a share point or folder, you create a list of access control entries (ACEs). Each ACE lets you set 17 permissions with allow, deny, and static inheritance. This allows you to have fine-grain control over access permissions, something that you can't do 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.

Note: You can't explicitly configure ACL permissions for files. However, because files can inherit ACL permissions from their parent folder, you can set permissions for files by setting them for the parent folder and propagating them to descendant files.

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

1 Open Workgroup Manager and click Sharing.

2 Click All and select the share point or folder.

3 Click Access.

4 Click Users & Groups to open the Users & Groups drawer.

5 Drag groups and users in the order you want them in the Access Control List.

Note: 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 grant the same user editing permissions are ignored. In addition, the ACEs in the Access Control List take precedence over the standard permissions. For more information about permissions, see "Rules of Precedence" on page 24.

By default, each new ACE gives the user or group full read and inheritance permissions. To change ACE settings, see "Editing ACEs" on page 45.

6 Click Save.

Note: ACLs are enabled by default at the volume level. If they're not, you can enable ACLs by clicking All in the Sharing pane of Workgroup Manager, selecting the volume on which you want to enable ACLs, selecting "Enable Access Control Lists on this volume" in the General pane, and clicking save.

Changing Apple File Settings for a Share Point

You can use Workgroup Manager to choose whether a share point is available via AFP and to change settings such as the share point name that AFP clients see, whether guest access is allowed, or the permissions model for new items.

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 Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols and choose Apple File Settings from the pop-up menu.

4 To provide AFP access to the share point, select "Share this item using AFP."

5 To allow unregistered users to access the share point, select "Allow AFP guest access."

For greater security, don't select this item.

6 To change the name that clients see when they browse for and connect to the share point using AFP, type 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.

7 If using only POSIX permissions, choose a default permissions option for new files and folders.

To have new or copied items keep their original privileges while inheriting the user and group ID of the user who creates or copies them, select "Use Standard POSIX behavior."

To have new or copied items adopt the privileges of the enclosing folder, select "Inherit permissions from parent."

Note: Don't select the "Inherit permissions" option for share points that contain home directories.

8 Click Save.

From the Command Line

You can also change AFP settings for a share point using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Windows (SMB/CIFS) Settings for a Share Point

You can use Workgroup Manager to set whether a share point is available via SMB/CIFS and to change settings such as the share point name that SMB/CIFS clients see, whether guest access is allowed, whether opportunistic locking is allowed, and the default privileges for new items. For more information about opportunistic locking, see the chapter on administering Windows users, groups, computers, and share points in the Windows services administration guide.

To change the settings of an SMB/CIFS share point:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols (on the right) and choose Windows File Settings from the pop-up menu.

4 To provide SMB/CIFS access to the share point, select "Share this item using SMB/CIFS."

5 To allow unregistered users access to the share point, select "Allow SMB/CIFS guest access."

For greater security, don't select this item.

6 To change the name that clients see when they browse for and connect to the share point using SMB/CIFS, type a new name in the "Custom SMB/CIFS name" field.

Changing the custom SMB/CIFS name doesn't affect the name of the share point itself, only the name that SMB/CIFS clients see.

7 To allow clients to use opportunistic file locking, select "Enable oplock."

To have clients use standard locks on server files, select "Enable strict locking."

8 If 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.

9 Click Save.

From the Command Line

You can also change a share point's SMB/CIFS settings using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing FTP Settings for a Share Point

You can use Workgroup Manager to set whether a share point is available via FTP and to change settings such as whether guest access is allowed and the share point name that FTP clients see.

To change the settings of an FTP share point:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols and choose FTP Settings from the pop-up menu.

4 To make the share point available to FTP clients, select "Share this item using FTP."

5 Select "Allow FTP guest access" to allow anonymous FTP users to open this item.

For greater security, don't select this item.

6 To change the name clients see when they browse for and connect to the share point using FTP, type 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.

7 Click Save.

From the Command Line

You can also change a share point's FTP settings using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

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 Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols and choose NFS Export Settings from the pop-up menu.

4 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" and click Add to specify the IP addresses of computers that can access the share point.

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

Important: Make sure that the subnet address you enter is the actual IP network address that corresponds to the subnet mask you chose (not just one of the client addresses). Otherwise, your clients will be unable to access the share point.

A network calculator can help 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. Calculators are available on the Web; use Sherlock or Google to search for "subnet calculator."

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 can discover that the mask 255.255.255.128 applied to any address in this range defines a subnet with network address 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 Workgroup Manager 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 allow unlimited (and unauthenticated) access to the share point, choose "World."

Note: If you export more than one NFS share point to "World," only the last export is available to clients. Don't create more than one NFS world export on a single server volume.

5 Select "Map Root user to nobody" if you want the root user on a remote client to have only minimal privileges to read, write, and execute commands.

6 Select "Map All users to nobody" if you want all users to have minimal privileges to read, write, and execute.

7 Select "Read-only" if you don't want client users to be able to modify the contents of the shared item in any way.

8 Click Save.

File and file range locking (standard POSIX advisory locks) are enabled by default for NFS share points in Mac OS X Server.

From the Command Line

You can also set up an NFS share point by using the `niutil` command in Terminal to add an entry to the NetInfo /exports directory. For more information, see the file services chapter of the command-line administration guide.

Resharing NFS Mounts as AFP Share Points

Resharing NFS mounts (NFS volumes that have been exported to the Mac OS X Server) as AFP share points allows clients to access NFS volumes using the secure authentication of an AFP connection. Resharing NFS mounts also allows Mac OS 9 clients to access NFS file services on traditional UNIX networks.

To reshare an NFS mount as an AFP share point:

1. 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.

   Restrict the export to the single AFP server (seen as the client to the NFS server). For even greater security, you can set up a private network for the AFP-to-NFS connection.

2. Click the add share button beneath the list of share points and enter the URL of the NFS server you intend to reshare.

   This is the URL users will enter in the Connect To Network window to connect to the reshared NFS server. For example, to connect to the reshared NFS mount "widgets" on the root level of the server corp1, use the following URL:

   nfs://corp1/widgets

3. Click OK.

   Workgroup Manager creates the NFS mount point.

4. Follow steps 1 through 3 for each NFS volume you want to reshare.

5. Use the Sharing pane of Workgroup Manager to share the NFS mounts as AFP share points.

   The NFS mounts appear as normal volumes in the All list. (You can also share the NFS mounts using SMB/CIFS and FTP, but it's recommended that you use only AFP.) You can change privileges and ownership, but not enable quotas (quotas work only on local volumes). However, if quotas are enabled on the NFS server, they should apply to the reshared volume as well.

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 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 database. Be sure you create these records in the same shared domain in which the user and computer records exist.

Note: All users have guest access to network automounted AFP share points. Authenticated access is allowed only for a user's own home directory or if you have Kerberos set up to support single sign-on.

To set up a network mount:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Network Mount (on the right).

4 Choose the directory domain that contains your users and computers from the Where pop-up menu.

If the correct directory is already chosen, click the lock to authenticate.

5 Choose the sharing protocol (AFP or NFS) from the Protocol pop-up menu.

Note: Make sure that AFP guest access is enabled in the Protocols pane for automounted AFP share points to work.

6 Choose how you want the share point to be used and mounted on client computers.

User Home Directories: the home directories on the share point are listed on a user's computer in /Network/Servers (in Servers inside the Network globe in the Finder).

Note: Share points used for home directories should be named using only US ASCII characters. Don't use multibyte encoding or accented characters.

Shared Applications: the share point appears on the user's computer in /Network/Applications (in Applications inside the Network globe in the Finder).

Shared Library: the share point appears in /Network/Library (in Library inside the Network globe in the Finder).

"Custom mount path": the share point appears in the directory you specify. You must make sure that this directory exists on the client computer before the share point can be mounted.

7 Click Save.

Managing Share Points

This section describes typical day-to-day tasks you might perform after you have set up share points on your server. Initial setup information appears in "Setting Up a Share Point" on page 33.

Disabling a Share Point

To stop sharing a particular share point, you use the Sharing module of Workgroup Manager to remove it from the Share Points list.

You may want to notify users that you are removing a share point so that they know why the share point is no longer available.

Note: Don't delete or rename a share point in the Finder without unsharing it in Workgroup Manager first.

To remove a share point:

1 Open Workgroup Manager and click Sharing.

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

3 Click General and deselect "Share this item and its contents."

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

From the Command Line

You can also disable a share point by using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Disabling a Protocol for a Share Point

You can use the Sharing module of Workgroup Manager to stop sharing a share point using a particular protocol and still allow sharing to continue via other protocols.

To stop sharing via a particular protocol:

1 Open Workgroup Manager and click Sharing.

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

3 Click Protocols and choose settings for the protocol from the pop-up menu.

4 Deselect "Share this item using..."

You can disable a protocol for all share points by stopping the underlying service that provides support for the protocol. For help, see "Stopping AFP Service" on page 60; "Starting and Stopping NFS Service" on page 72; or "Stopping FTP Service" on page 86.

From the Command Line

You can also disable a protocol for a share point by using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing Share Points

You can use the Sharing module of Workgroup Manager to view share points and their contents.

To view share points on a server:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points.

   Select an item in the list to see its contents. Use the scroll bar at the bottom to move up or down in the directory hierarchy.

From the Command Line

You can also view share points and their contents by using the `sharing` and `ls` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing a Share Point's Path

You can view the path to a share point in Workgroup Manager by moving the mouse over the name of the share point in the Share Points list.

To view a share point's path:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points.
3. Move the mouse pointer over the share point.

   A help tag appears displaying the path.

Note: Help tags will only appear over share point names in the first column.

Viewing Share Point Settings

You can use Workgroup Manager to view the sharing and privilege settings for a share point.

To view sharing and privileges for a share point:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points and select the share point you want to view.
3. Click Access to view the privileges for the share point.
4. Click Protocols and use the pop-up menu to see the protocol settings for the item.
5. Click Network Mount to see the automatic mount settings.

From the Command Line

You can also view share point settings using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing Share Point Access Privileges

Managing access privileges to share points involves the following:

- "Changing Standard Permissions" on page 43
- "Adding ACEs to ACLs" on page 44
- "Removing ACEs" on page 44
- "Editing ACEs" on page 45
- "Removing a Folder's Inherited ACEs" on page 45
- "Making a Folder's Inherited ACE Entries Explicit" on page 46
- "Propagating Permissions" on page 46
- "Removing a File's ACL" on page 47
- "Applying ACL Inheritance to a File" on page 47
- "Determining User or Group Permissions to a File or Folder" on page 47

Changing Standard Permissions

You use Workgroup Manager to view and change the standard privileges for a share point.

To change standard privileges for a share point:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points and select the share point you want to update.
3. Click Access.
4. Change the owner and group of the shared item by typing names into those fields or by dragging names from the Users & Groups drawer. You can open the drawer by clicking "Users & Groups."
5. Use the pop-up menus next to the fields to change the permissions for the Owner, Group, and Everyone.

   Everyone is any user who is not the owner and does not belong to the group but can log in to the file server: other registered users and guests.

From the Command Line

You can also change a share point's privileges using the `chmod`, `chgrp`, and `chown` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Adding ACEs to ACLs

You control access to a share point by adding or removing access control entries (ACEs) to the share point's access control list (ACL). Each ACE defines the access permissions for a user or a group.

To add an ACE to an ACL:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Access.

4 Click Users & Groups to open the Users & Groups drawer.

5 Drag groups and users in the order you want them in the Access Control List.

6 Click Save.

By default, each new ACE gives the user or group full read permissions. In addition, the four inheritance options are selected. To change ACE settings, see "Editing ACEs" on page 45.

From the Command Line

You can also add ACEs using the `chmod` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Removing ACEs

You control access to a share point by adding or removing access control entries (ACEs) to the share point's access control list (ACL). Each ACE defines the access permissions for a user or a group.

To delete an ACE from an ACL:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Access.

4 Select the ACE.

You can select only one ACE at a time.

5 Click the "Remove selected item" button.

6 Click Save.

From the Command Line

You can also remove ACEs using the `chmod` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Editing ACEs

If you need change the settings of an access control entry (ACE) to allow or restrict what a user or group can do in a share point, use the "Edit selected item" button in the Access pane of the Sharing pane in Workgroup Manager.

To edit an ACE:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points and select the share point.
3. Click Access.
4. Select the entry.
5. Click the "Edit selected item button" (button with a pencil icon below the list).
6. Select the permissions type from the pop-up menu.
7. Select permissions in the Permissions list.
8. Click OK.
9. Click Save.

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

- Full Control—Selects all 17 permissions
- Read and Write—Selects only the Read and Write permissions
- Read—Selects only the Read permissions
- Write—Selects only the Write permissions
- Custom—Lets you specify the permissions you want to select (this is the equivalent of clicking the "Edit selected item button")

For more information about permissions and permission types, see "Access Control Entries" on page 21.

Removing a Folder's Inherited ACEs

If you don't want to apply inherited access control entries (ACEs) to a folder or a file, you can remove these entries using the "Remove inherited entries" command.

To remove a folder's inherited ACEs:

1. Open Workgroup Manager and click Sharing.
2. Click All and select the file or folder.
3. Click Access.
4. Choose "Remove inherited entries" from the Action menu (bottom right).
5. Click Save.

Workgroup Manager automatically removes the inherited ACEs.

Note: Inherited ACEs appear dimmed unless you chose to make them explicit, as described in "Making a Folder's Inherited ACE Entries Explicit" on page 46.

From the Command Line

You can also remove inherited ACEs using the `chmod` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Making a Folder's Inherited ACE Entries Explicit

Inherited access control entries (ACEs) appear dimmed in the Access Control List in the Access pane of the Sharing pane of Workgroup Manager and you can't edit them. To modify these ACEs for a particular folder, first make them explicit using the "Make inherited entries explicit" command. Then you can edit them.

To make a folder's inherited ACEs explicit:

1. Open Workgroup Manager and click Sharing.
2. Click All and select the folder.
3. Click Access.
4. Choose "Make inherited entries explicit" from the Action menu (bottom right).
5. Click Save.

Workgroup Manager automatically makes the inherited ACEs no longer dim. Now you can edit them.

Propagating Permissions

Workgroup Manager allows you specify what permissions to propagate to all descendant files and folders. In the case of standard permissions, you can specify which of the following information to propagate to descendants:

- Owner name
- Group name
- Owner permissions
- Group permissions
- Everyone permissions

The ability to select which information to propagate gives you more fine-grain control over who can access files and folders. In the case of access control list (ACL) permissions, you can only propagate the entire ACL. You can't propagate individual ACEs.

To propagate folder permissions:

1. Open Workgroup Manager and click Sharing.
2. Click All and select the folder.
3. Click Access.
4. Choose "Propagate permissions" from the Action menu (bottom right).
5. Select the permissions to propagate.

Workgroup Manager automatically propagates the selected permissions to all descendants.

Removing a File's ACL

To remove a file's inherited access control entries (ACEs), use the "Remove access control list" command in Workgroup Manager.

Note: Because a file's ACEs are always inherited, they appear dimmed in the file's ACL.

To remove a file's ACL:

1 Open Workgroup Manager and click Sharing.

2 Click All and select the file.

3 Click Access.

4 Choose "Remove access control list" from the Action menu (bottom right).

5 Click Save.

Workgroup Manager automatically removes all ACEs from the file's ACL. The only permissions that now apply are the standard permissions.

From the Command Line

You can also remove a file's ACL using the `chmod` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Applying ACL Inheritance to a File

If you removed a file's access control list (ACL) and want to restore it, use the "Apply inheritance to selected file" command in the Access pane of the Sharing pane of Workgroup Manager.

To apply inheritance to a file:

1 Open Workgroup Manager and click Sharing.

2 Click All and select the file.

3 Click Access.

4 Choose "Apply inheritance to selected file" from the Action menu (bottom right).

5 Click Save.

Determining User or Group Permissions to a File or Folder

Workgroup Manager provides a handy tool, the Effective Permission Inspector, that you can use to instantly determine the permissions that a user or a group has to a file or folder. Finding out these permissions without this tool can be tricky and time-consuming in some cases.

To determine user or group permissions to a file or folder:

1. Open Workgroup Manager and click Sharing.
2. Click All and select a file or a folder.
3. Click Access.
4. Choose "Show Effective Permission Inspector" from the Action menu (bottom right).

   Note: In the inspector, all permissions and inheritance settings appear dimmed to indicate that you can't edit them.

5. Drag a user or group from the Users & Groups drawer to the "File/Folder name" field.

   To open the drawer, click Users & Groups. If you don't see a recently created user or group, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences and change the value of the "Auto-refresh Sharing every" field.

   After dragging the user from the drawer, the inspector shows the permissions the user or group has to the selected file or folder. A selected entry means that the user or group has the indicated permission (equivalent to allow). A deselected entry means the opposite (equivalent to deny).

6. Close the inspector window when done.

Changing the Protocols Used by a Share Point

You can use the Protocols pane of Workgroup Manager to change the protocols available for accessing a share point.

To change the protocols for a share point:

1. Open Workgroup Manager and click Sharing.
2. Click Share Points and select the share point you want to change.
3. Click Protocols.
4. Use the pop-up menu to choose the protocols you want to change.

   See the following sections for descriptions of the protocol settings:
   - "Changing Apple File Settings for a Share Point" on page 35
   - "Changing Windows (SMB/CIFS) Settings for a Share Point" on page 36
   - "Changing FTP Settings for a Share Point" on page 37
   - "Exporting an NFS Share Point" on page 38

From the Command Line

You can also change a share point's protocol settings using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing NFS Share Point Client Access

You can use the Protocols pane of Workgroup Manager to restrict the clients that can access an NFS export.

To change authorized NFS clients:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the NFS share point.

3 Click Protocols and choose NFS Export Settings from the pop-up menu.

4 To limit clients to specific computers, choose Client and click Add to specify the IP addresses of computers that can access the share point. To remove a client, select an address and click Remove.

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

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

5 Click Save.

Allowing Guest Access to a Share Point

You can use Workgroup Manager to allow guest users (users not defined in the directories used by your server) to connect to specific share points.

To change guest access privileges for a share point:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols and use the pop-up menu to choose the protocol you're using to provide access to the share point.

4 Select the "Allow guest access" option.

5 Click Save.

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

From the Command Line

You can also enable guest access to a share point using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Setting Up a Drop Box

A drop box is a shared folder with ACL permissions set so that certain users can only copy files into the folder, but can't see its contents. If you use only POSIX permissions, you can set them to allow anyone the ability to copy files into 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 within an AFP share point.
2. Open Workgroup Manager and click Sharing.
3. Click Share Points and select the folder in the AFP share point that you want to use as a drop box.
4. Click Access.
5. Set write only permissions using POSIX permissions or a combination of POSIX permissions and Access Control Entries (ACEs).

   - To create a drop box using standard permissions, set Write Only permissions for Owner, Group, and Everyone. For more information on setting standard permissions, see "Setting Standard Permissions" on page 34.

     Note: For greater security, don't allow access to everyone—assign None to Everyone.

   - To create a drop box, add two types of ACEs:
     - For those uses who should be able to only copy items into a drop box but not see its contents, add ACEs that deny them Administration and Read permissions and allow only "Create File (Write Data)" and "Create Folder (Append Data)" permissions.
     - For users who should have full control of the drop box, add ACEs to give them full Administration, Read, and Write permissions.

     For more information on setting ACL permissions, see "Setting ACL Permissions" on page 34.
6. Click Save.

From the Command Line

You can also set up a drop box using the `mkdir` and `chmod` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Using Workgroup Manager With Mac OS X Server v10.1.5

Workgroup Manager is available only on Mac OS X Server v10.2 or later. If you want to use Workgroup Manager to edit account information on a computer running Mac OS X Server v10.1.5, you must access that server remotely from a computer running Mac OS X Server v10.2 or later and log in as a root user.

To log in to a remote server as a root user with Workgroup Manager:

1. In Workgroup Manager, choose the shared domain of interest from the domain pop-up list below the toolbar.

   Alternatively, you can choose View Directories from the Server menu.
2. Use a root user name and password to log in.

If you are not logged in as a root user, you can't make changes using Workgroup Manager.

If possible, you should upgrade servers on your network to use Mac OS X Server version 10.2 or later.

Note: You wont be able to use Workgroup Manager to create share points on a computer running Mac OS X Server v10.1.5.

Setting SACL Permissions

Service access control lists (SACLs) allow you to specify which users and groups have access to AFP, FTP, and Windows file services.

To set SACL permissions for a file service:

1 Open Server Admin.

2 Select the server from the Computers & Services list.

3 Click Settings.

4 Click Access.

5 Select "Use same access for all services" to restrict access to all services or deselect this option to set access permissions per service.

6 If you have deselected "Use same access for all services," select a service from the Service list.

7 Click "Allow all users and groups" to provide unrestricted access to services.

If you want to restrict access to certain users and groups:

a Select "Allow only users and groups below."
b Click the Add (+) button to open the Users & Groups drawer.
c Drag users and groups from the Users & Groups drawer to the list.

8 Click Save.

AFP Service

3

This chapter describes how to set up and manage AFP service in Mac OS X Server.

AFP (Apple Filing Protocol) service allows Mac OS clients to connect to your server and access folders and files as if they were located on their own computers. Non-Mac OS clients can also connect to your server over AFP using third-party AFP client software.

AFP service uses version 3.2 of AFP, which supports new features such as Unicode file names, ACLs, and 64-bit file sizes. Unicode is a standard that assigns a unique number to every character regardless of language or the operating system used to display the language.

Kerberos Authentication

Apple file service 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 utilizes Generic Security Services Application Programming Interface (GSSAPI) authentication protocol to support Kerberos v.5. You specify the authentication method using the Access pane of the AFP service settings in Server Admin. See "Changing Access Settings" on page 56. For more information on setting up Kerberos, see the Open Directory administration guide.

Automatic Reconnect

Mac OS X Server provides the ability to automatically reconnect Mac OS X clients that have become idle or gone to sleep. When clients become idle or go to sleep, the Mac OS X Server disconnects those clients to free up server resources. Mac OS X Server can save Mac OS X client sessions, however, allowing these clients to resume work on open files without loss of data. You configure this setting in the Idle Users pane of the AFP service configuration window in Server Admin. See "Changing Idle User Settings" on page 58.

Find By Content

Mac OS X clients can use Sherlock to search the contents of AFP servers. This feature enforces privileges so that only files to which the user has access are searched.

AppleTalk Support

AFP service no longer supports AppleTalk as a client connection method. While AppleTalk clients will see AFP servers in the Chooser, they must use TCP/IP to connect to these servers. See "Mac OS X Clients" on page 66 and "Mac OS 8 and Mac OS 9 Clients" on page 67 for more information.

Apple File Service Specifications

- Maximum number of connected users, depending on your license agreement: Unlimited (hardware dependent)
- Maximum volume size: 2 terabytes
- TCP port number: 548
- Location of log file or files: /Library/Logs/AppleFileService
- Bonjour registration type: afpserver

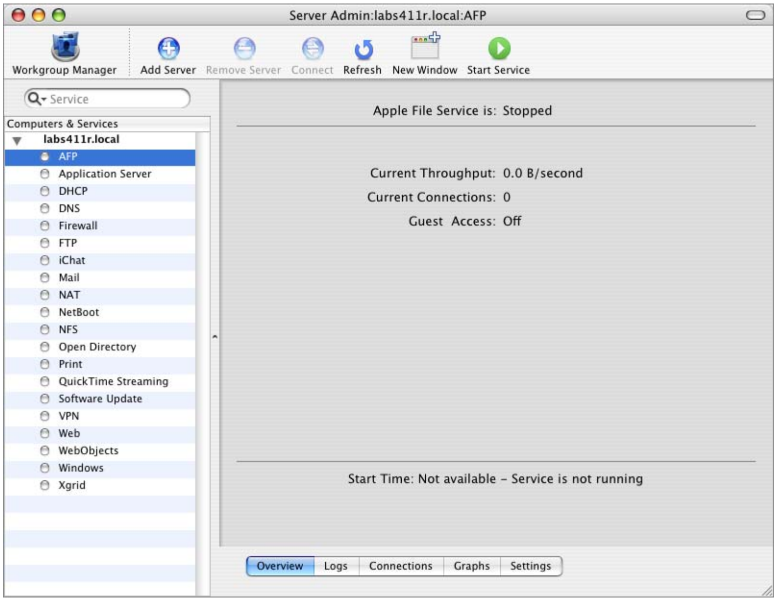
Setting Up AFP Service

If you allowed the Server Assistant to start AFP service when you installed Mac OS X Server, you don't have to do anything else. However, you should check to see if the default service settings meet your needs. The following section steps you through each of the Apple file service settings.

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

- **General.** Set information that identifies your server, enable automatic startup, and create a login message for Apple file service.
- **Access.** Set up client connections and guest access.
- **Logging.** Configure and manage logs for Apple file service.
- **Idle users.** Configure and administer idle user settings.

The following sections describe the tasks for configuring these settings. A fifth section tells you how to start up Apple file service after you've completed its configuration.



Apple File Service is: Stopped

Current Throughput: 0.0 B/second
Current Connections: 0
Guest Access: Off

Start Time: Not available – Service is not running

Configuring General Settings

You use the General pane of AFP service settings to enable automatic startup, enable browsing with Network Service Location or AppleTalk, and create a login greeting for your users.

To configure AFP service General settings:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Settings, then click General.

3 To advertise the AFP share point using both Network Service Location (NSL) and Bonjour, select "Enable Bonjour registration."

This option lets clients browse for the share point using the Mac OS X "Connect to Server" command or the Mac OS 9 Network Browser.

For NSL registration to work, you must also enable IP multicasting on your network routers. See the network services administration guide for more information about Service Location Protocol (SLP) and IP multicasting.

4 To allow Mac OS 8 and Mac OS 9 clients to find your file server using the Chooser, select "Enable browsing with AppleTalk."

For Chooser browsing to work, AppleTalk must be enabled on both the client computer and the server. Clients can then see the server in the Chooser, but will need to connect using TCP/IP.

5 If you have Mac OS 8 and Mac OS 9 clients with special language needs, choose the appropriate character set from the "Encoding for older clients" pop-up menu.

When Mac OS 9 and earlier clients are connected, the server converts file names from the system's UTF-8 to the chosen set. This has no effect on Mac OS X client users.

6 In the Logon Greeting field, type the message you want users to see when they connect.

Note: The message does not appear when a user logs in to his or her home directory.

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

8 Click Save.

From the Command Line

You can also change the AFP service settings using the `serveradmin` command in Terminal or by modifying the AFP preferences file. For more information, see the file services chapter of the command-line administration guide.

Changing Access Settings

The Access pane of AFP Settings in Server Admin lets you control client connections and guest access.

To configure AFP service Access settings:

1 Open Server Admin and select AFP in the Computers & Services list.

2 Click Settings, then click Access.

3 Choose the authentication method you want to use: Standard, Kerberos, or Any Method.

4 To allow unregistered users to access AFP share points, select "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 allow guest access for Apple file service in general, you can still selectively enable or disable guest access for individual share points.

5 To allow clients to connect using secure AFP (using SSH), select "Enable secure connections."

6 To allow an administrator to log in using a user's name with an administrator password (and thereby experience the AFP service as the user would), select "Enable administrator to masquerade as any registered user."

7 To restrict the number of simultaneous client connections, click next to the number field for clients or guests and type 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, then a maximum of 10 users can connect at one time.

The maximum number of guests cannot exceed the maximum number of total client connections allowed.

8 Click Save.

From the Command Line

You can also change the AFP access settings using the `serveradmin` command in Terminal or by modifying the AFP preferences file. For more information, see the file services chapter of the command-line administration guide.

Changing Logging Settings

You use the Logging pane of the Apple File Service settings in Server Admin to configure and manage service logs.

To configure Apple file service Logging settings:

1 Open Server Admin and select AFP in the Computers & Services list.

2 Click Settings, then click Logging.

3 To keep a record of users who connect to the server using AFP, select "Enable Access log."

4 To periodically close and save the active log and open a new one, select "Archive every __ days" and type the number of days after which the log is archived.

5 Select the events that you want Apple file service to log.

An entry is added to the log each time a user performs one of the actions you select.

Consider available disk space when you choose the number of events to log. The more events you choose, the larger the log file.

6 To specify how often the error log file contents are saved to an archive, select "Error Log: Archive every __ days" and type the number of days.

7 Click Save.

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.

You can keep the archived logs for your records or delete them to free disk space when they're no longer needed. The default setting is 7 days. 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

You can also change the AFP service logging settings using the `serveradmin` command in Terminal or by modifying the AFP preferences file. For more information, see the file services chapter of the command-line administration guide.

Changing Idle User Settings

You use the Idle Users pane of Apple File Service settings 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 a predefined period of time.

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

To configure idle user settings:

1 Open Server Admin and select AFP in the Computers & Services list.

2 Click Settings (near the bottom of the window), then click Idle Users.

3 To allow client computers to reconnect after sleeping for a certain time, select "Allow clients to sleep __ hour(s)—will not show as idle" and type the number of hours clients can sleep and remain reconnected to the server.

4 To specify the idle time limit, select "Disconnect idle users after __ minutes" and type the number of minutes after which an idle computer should be disconnected.

A sleeping Mac OS X version 10.2 (and later) client will be able to resume work on open files within the limits of the "Allow clients to sleep" setting.

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

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

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

7 Click Save.

From the Command Line

You can also change the AFP service idle user settings using the `serveradmin` command in Terminal or by modifying the AFP preferences file. For more information, see the file services chapter of the command-line administration guide.

Starting AFP Service

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

To start Apple file service:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Start Service (near the top of the window).

   The service will run until you stop it and will restart automatically if your server is restarted for any reason.

From the Command Line

You can also start the AFP service using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing AFP Service

This section tells you how to perform day-to-day management tasks for AFP service once you have it up and running.

Checking Service Status

You can use Server Admin to check the status of AFP service.

To view AFP service status:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Overview (near the bottom of the window) to see whether the service is running, when it started, its throughput and number of connections, and whether guest access is enabled.
3. Click Logs to review the access and error logs.

   Use the Show pop-up menu to choose which log to view.
4. Click Connections to see a list of connected users.

   The list includes the user name, type of connection, user's IP address or domain name, duration of connection, and the time since the last data transfer (idle time).
5. Click Graphs to see graphs of connected users or throughput.

   Use the pop-up menu to choose which graph to view. Adjust the time scale using the slider at the bottom of the pane.

From the Command Line

You can also check the status of the AFP service process using the `ps` or `top` commands in Terminal, or look at the log files in /Library/Logs/AppleFileService using the `cat` or `tail` command. For more information, see the file services chapter of the command-line administration guide.

Viewing Service Logs

You 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 select AFP in the Computers & Services list.
2. Click Logs and use the Show pop-up menu to choose between the access and error logs.

To enable logging, click Settings (near the bottom of the window), then click Logging.

From the Command Line

You can also view the AFP service logs in /Library/Logs/AppleFileService using the `cat` or `tail` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Stopping AFP Service

You use Server Admin to stop AFP service.

Important: When you stop AFP service, connected users may lose unsaved changes in open files.

To stop Apple file service after warning users:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Connections (near the bottom of the window), then click Stop.
3. Type the length of time the server will wait before stopping service.
4. Type a message in the Additional Message field if you want users to know why they must disconnect.

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

From the Command Line

You can also stop the AFP service immediately using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Enabling NSL and Bonjour Browsing

You can register the service with Network Service Locator (NSL) and Bonjour to allow users to find the server by browsing through available servers. Otherwise, users who cannot browse via AppleTalk (see below) must type the server's host name or IP address when connecting.

To register with NSL and Bonjour:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click General, select "Enable Bonjour registration," and click Save.

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

   To take advantage of NSL registration, you must also enable and configure Service Location Protocol (SLP) service on your network router.

From the Command Line

You can also set the AFP service to register with NSL and Bonjour using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Enabling AppleTalk Browsing

If you enable browsing with AppleTalk, Mac OS 8 and 9 users can see your servers and other network resources using the Chooser.

Important: AppleTalk must be enabled both on the user's computer and on the server. On the server, you can use the Network pane of System Preferences.

To enable browsing via AppleTalk:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click General and select "Enable browsing with AppleTalk."
3. Click Save.

From the Command Line

You can also set the AFP service to enable AppleTalk browsing using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Limiting Connections

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 select AFP in the Computers & Services list.
2. Click Settings, then click Access and look under "Maximum Connections."
3. Click the button next to the number field following "Client Connections (Including Guests)" and type the maximum number of connections you want to allow.
4. Next to "Guest connections," enable the number field and type the maximum number of guests you want to allow.
5. Click Save.

The guest connections limit is based on the client connections limit, and guest connections count against 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.

From the Command Line

You can also set the AFP service connections limit using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Keeping an Access Log

The access log can record 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 select AFP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Logging.
3. Select "Enable access log."
4. Select the events you want to record.

   Consider your server's disk size when choosing events to log. The more events you choose, the larger the log file.

To view the log, open Server Admin, select AFP, and click Logs. Log files are stored in /Library/Logs/AppleFileService.

From the Command Line

You can also set the AFP service to record logs using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Archiving AFP Service Logs

You can periodically save the active logs and open new logs.

To set how often logs are archived:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Logging.
3. Select "Archive every __ days" and type the number of days to specify how often the log file contents are saved to an archive.
4. Select "Error Log: Archive every __ days" and type the number of days to specify how often the error log file contents are saved to an archive.
5. Click Save.

   The server closes the active log at the end of each archive period, renames it to include the current date, then opens a new log file. You can keep the archived logs for your records or delete them to free disk space when they are no longer needed. The default setting is 7 days.

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

You can also set the AFP service log archival interval using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Disconnecting a User

You use Server Admin to disconnect users from the Apple file server.

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

To disconnect a user:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Connections.
3. Select the user and click Disconnect.
4. Enter the amount of time before the user is disconnected and type a disconnect message.

   If you don't type a message, a default message appears.
5. Click Disconnect.

Disconnecting Idle Users Automatically

You can set AFP service to automatically 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 select AFP in the Computers & Services list.

2 Click Settings (near the bottom of the window), then click Idle Users.

3 To allow client computers to reconnect after sleeping for a certain time, select "Allow clients to sleep __ hour(s)—will not show as idle" and type 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.

4 To specify the idle time limit, select "Disconnect idle users after __ minutes" and type the number of minutes after which an idle computer should be disconnected.

A sleeping Mac OS X version 10.2 (and later) client will be able to resume work on open files within the limits of the "Allow clients to sleep" setting.

5 To prevent particular classes of users from being disconnected, select them under "Except."

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

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

7 Click Save.

From the Command Line

You can also change the AFP service idle user settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Sending a Message to a User

You use Server Admin to send messages to clients using AFP service.

To send a user a message:

1 Open Server Admin and select AFP in the Computers & Services list.

2 Click Connections and select the user's name in the list.

3 Click Send Message.

4 Type the message and click Send.

Note: This communication is one way; users cannot reply to the message received from Server Admin.

Allowing Guest Access

Guests are users who can see information on your server without using a name or password to log in. For better security, don't allow guest access. After enabling guest access for the service, you'll need to enable guest access for specific share points. See "Allowing Guest Access to a Share Point" on page 49.

To enable guest access:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Access.
3. Select "Enable Guest access."
4. Under the "Maximum guest connections" option:

   Select Unlimited if you don't want to limit the number of guest users who can be connected to your server at one time.

   Enter a number if you want to limit how many client connections can be used by guests.
5. Click Save.

From the Command Line

You can also set the AFP service to allow guest access using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Creating a Login Greeting

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

To create a login greeting:

1. Open Server Admin and select AFP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click General.
3. Type a message in the Logon Greeting field.
4. To prevent users from seeing the message more than once, select "Do not send same greeting twice to the same user."

   If you change the message, users will see the new message the next time they connect to the server.
5. Click Save.

From the Command Line

You can also change the AFP service greeting using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Supporting AFP Clients

This section describes how client computers can access Mac OS X Server AFP share points.

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

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

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 or Network Service Location, you can browse for it in the Network globe in the Finder.

Note: Apple file service doesn't support AppleTalk connections, so clients need to use TCP/IP to access file services. You can use AppleTalk to find Apple file servers, but the connection must be made using TCP/IP.

To connect to the Apple file server from 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 and select the server in the list (if it appears there).
   - Type the DNS name of the server in the Address field. You can enter DNS names in any of the following forms:

     ```
     server
     afp://server
     afp://server/sharepoint
     ```
   - Type the server's IP address in the Address field.
3. Click Connect.
4. Type your user name and password or select Guest, then click Connect.
5. Select the share point you want to use and click OK.

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

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

To set a Mac OS X version 10.2.6 or earlier client computer to mount a server volume automatically:

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 client user logs in the next time, the server, if available, will be mounted automatically.

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

To set a Mac OS X version 10.3 client computer to mount a server volume automatically:

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

Mac OS 8 and Mac OS 9 Clients

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

- Mac OS 8 (version 8.6) or Mac OS 9 (version 9.2.2)
- TCP/IP
- AppleShare Client 3.7 or later

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

Connecting to the AFP Server from Mac OS 8 or Mac OS 9

Apple file service does not support AppleTalk connections, so clients need to use TCP/IP to access file services. You can use AppleTalk to find Apple file servers, but the connection must be made using TCP/IP. For this to work, AppleTalk Browsing must be enabled on the servers and the clients must have a valid TCP/IP configuration as well as the most recent version of the AppleShare Client software.

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

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

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

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

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

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

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

NFS Service

4

This chapter describes how to set up and manage the NFS file service in Mac OS X Server.

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

You can export a shared item to a set of client computers or to "World." Exporting an NFS volume to World means that anyone who can access your server can also access that volume.

Note: The NFS term for sharing is *export*. This guide, therefore, uses that term to be consistent with standard NFS terminology.

You use Server Admin to configure and manage NFS service. You also use the Sharing module of Workgroup Manager to set privileges and access levels for the share points or folders you want to export.

The NFS service doesn't support ACLs. The client filter access is based on only POSIX permissions.

Setup Overview

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

Step 1: Before you begin

Read "Before Setting Up NFS Service" on page 70 for issues you should keep in mind when you set up NFS service.

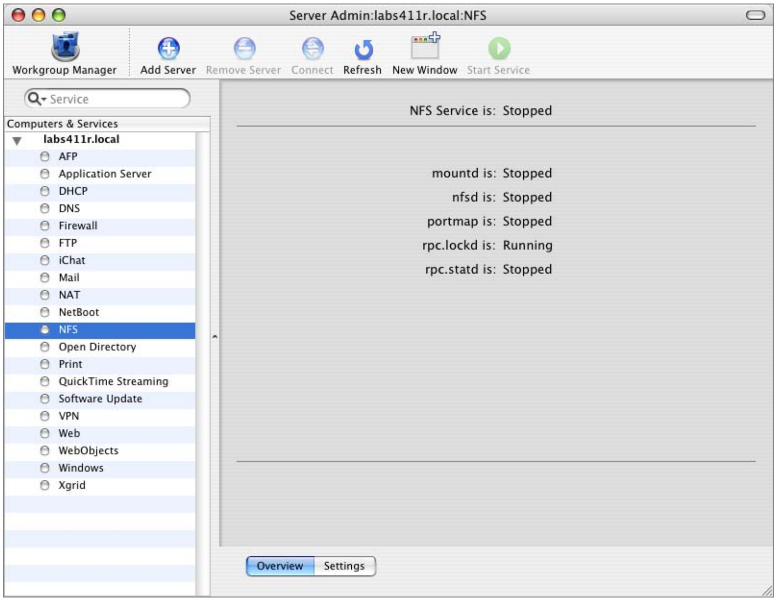
Step 2: Configure NFS settings

The NFS settings let you set the maximum number of daemons and choose how you want to serve clients—via TCP, UDP, or both. See "Configuring NFS Settings" on page 71.

Step 3: Create share points and share them using NFS

Use the Sharing module of Workgroup Manager to specify the share points you want to export (share) using NFS. You must explicitly configure a share point to use NFS in order for NFS users to be able to access the share point. See "Creating a Share Point" on page 33, "Exporting an NFS Share Point" on page 38, and "Automatically Mounting Share Points for Clients" on page 40.

You don't need to start or stop NFS service; when you export a share point, the service starts automatically. When you delete all exports, the service stops. To see if NFS service is running, open Server Admin, select NFS in the Computers & Services list, and click Overview.



NFS Service is: Stopped

mountd is: Stopped
nfsd is: Stopped
portmap is: Stopped
rpc.lockd is: Running
rpc.statd is: Stopped

Before Setting Up NFS Service

Be sure to consider the security implications of exporting in NFS before you set up NFS service. NFS was created for a secure networking environment, in which you can trust the client computer users and the people who administer the clients. Whereas access to Apple file service, Windows file sharing, and FTP service share points is controlled by authentication (user name and password), access to NFS shared items is controlled by the client software and file permissions.

NFS allows access to information based on the computer's IP address. This means that a particular client computer will have access to certain share points regardless of who is using the computer. Whenever that computer is started up, some volumes or folders are automatically mounted or made available, and anyone using that computer can access those volumes or folders.

With NFS, it's possible for a user to *spoof* ownership of another person's files. For example, if a file on the server is owned by a user with user ID 1234, and you export a folder that contains that file, someone on a remote computer can create a local user on the remote computer, give it a user ID of 1234, mount that folder, and have the same access to the folder's contents as the file's original owner.

You can take some steps to prevent this by creating unique user IDs and by safeguarding user information. If you have Internet access and plan to export to World, your server should be behind a firewall.

Setting Up NFS Service

You can use Server Admin to change some NFS service settings.

Configuring NFS Settings

The NFS settings let you set the maximum number of daemons and choose how you want to serve clients—via TCP, UDP, or both.

To configure NFS settings:

1 Open Server Admin and select NFS in the Computers & Services list.

2 Click Settings (near the bottom of the window).

3 Type a number in the "Use__server daemons" field to specify the maximum number of nfsd daemons you want to allow to run at one time.

An nfsd daemon is a server process that runs continuously behind the scenes and processes reading and writing requests from clients. The more daemons that are available, the more concurrent clients can be served. Typically, four to six daemons are adequate to handle the level of concurrent requests.

4 Choose how you want to serve data to your client computers.

Select both TCP and UDP unless you have a specific performance concern. TCP provides better performance for clients, and UDP puts a smaller load on the server.

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

User Datagram Protocol (UDP) is a connection-less transport protocol. UDP doesn't break data into packets, so it uses fewer system resources. It's more scalable than TCP, and a good choice for a heavily used server. Do not use UDP, however, if remote clients are using the service.

5 Click Save.

From the Command Line

You can also change the NFS service settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing NFS Service

This section tells you how to perform day-to-day management tasks for NFS service once you have it up and running.

Starting and Stopping NFS Service

When the server starts up, a startup script checks to see if any NFS exports are defined; if so, NFS starts automatically.

If NFS is not running and you add exports, wait a few seconds for the service to launch.

To stop NFS service:

- Delete all exports.

The nsfd daemons continue to run until the server is restarted.

From the Command Line

You can also stop the NFS service processes using the `kill` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing NFS Service Status

You use Server Admin to check the status of all Mac OS X Server devices and services.

To view NFS service status:

1 Open Server Admin and select NFS in the Computers & Services list.

2 Click Overview (near the bottom of the window).

The Overview pane tells you whether the service is running, and whether mountd, nfsd, portmap, rpc.lockd, and rpc.statd processes are running.

The mountd process handles mount requests from client computers (only one mountd process will appear in the status window if you've defined any exports).

The nfsd process responds to read/write requests from client computers that have mounted folders.

The portmap process allows client computers to find nfs daemons (always one process).

The rpc.lockd is a daemon that provides file and record-locking services in an NFS environment.

The rpc.statd cooperates with rpc.statd daemons on other hosts to provide a status monitoring service. If a local NFS service crashes and restarts, the rpc.statd daemon will notify the hosts being monitored at the time of the crash.

From the Command Line

You can also check the NFS service status using the `ps` or `serveradmin` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing Current NFS Exports

You can use the Terminal application to view a list of the current NFS exports.

To view current NFS exports:

- In Terminal, type `showmount -e`.

If this command does not return results within a few seconds, there are no exports and the process will not respond. Press Control-C to exit the showmount command and return to an active command line in your Terminal window.

FTP Service

5

This chapter describes how to set up and manage File Transfer Protocol (FTP) service in Mac OS X Server.

FTP (File Transfer Protocol) is a simple way for computers of any type to transfer files over the Internet. Someone using any 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.

FTP service in Mac OS X Server 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 these differences are described in the following sections.

A Secure FTP Environment

Most FTP servers restrict users to specific directories on the server. Users can see folders and files only in these directories, so the server is kept quite secure. Users cannot access volumes mounted outside the restricted directories, and symbolic links and aliases cannot reach outside these boundaries.

FTP service in Mac OS X Server expands the restricted environment to allow access to symbolic links while still providing a secure FTP environment. You can allow FTP users access to the FTP root directory, their home directory, or to any other directory on the server that you set up as an FTP share point.

A user's access to the FTP root directory, FTP share points, and their home directory is determined by the user environment you specify (as described in the following section) and by their access privileges.

Note: The FTP service enforces ACL permissions.

FTP Users

FTP supports two types of users:

- **Authenticated users.** These users have accounts on your server (and might even have their home directories 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 use the Accounts module of Workgroup Manager to review or set up authenticated users.
- **Anonymous users.** These users do not have accounts on your server. They are also called *guest* users (for example, in Workgroup Manager when you set up an FTP share point). An anonymous user can access the FTP directories on the server files using the common user name "anonymous" and their email address, which may be fictitious, as their password. You use the General pane of FTP service settings in Server Admin to allow anonymous access to your server.

The FTP Root Directory

The FTP root directory (or simply FTP root) is a portion of your server's disk space set aside for FTP users. When you first install the server software, the FTP root is set to /Library/FTPServer/FTPRoot. You can change the FTP root; see "Changing the FTP Root Directory" on page 87.

FTP User Environments

Mac OS X Server lets you choose from three different FTP environments that give users access to some combination of the FTP root directory, other FTP share points, and user home directories:

- FTP root and Share Points.
- Home Directory with Share Points
- Home Directory Only

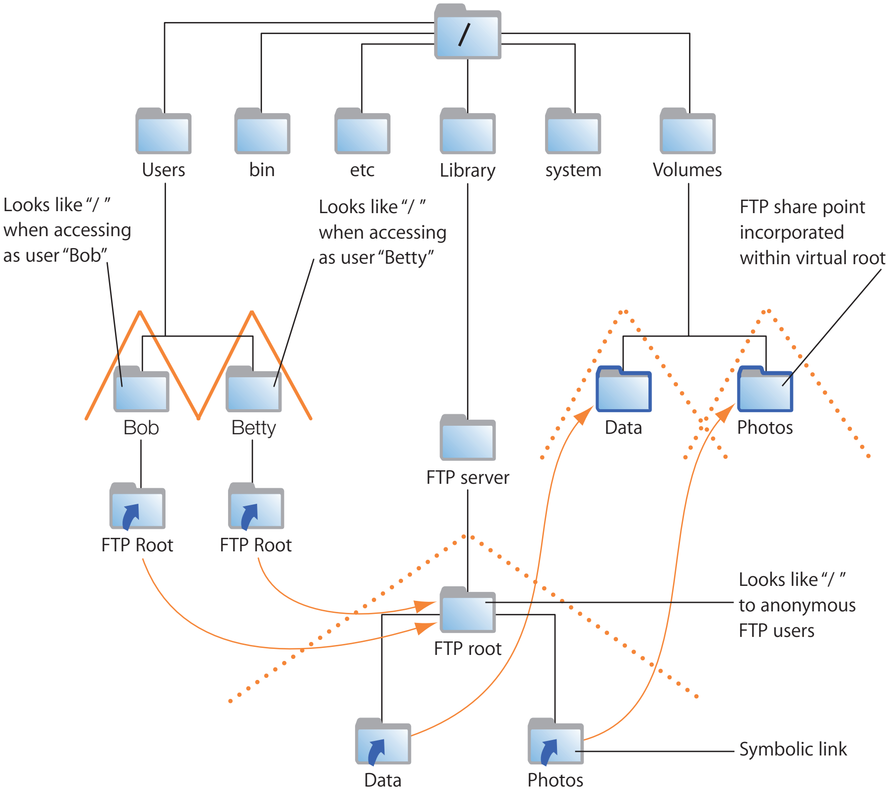
Share points in this case are any share points you have set up in Workgroup Manager to be shared using FTP.

Home directories are the home directories of users who have accounts on the server.

You can choose the user environment for your server in the Advanced pane of the FTP service settings in Server Admin. See "Changing Advanced Settings" on page 85.

FTP Root and Share Points

The "FTP Root and Share Points" option gives access—for both authenticated and anonymous users—to the FTP root and any FTP share points to which the users have access privileges, as shown in the following figure.


/
Users
bin
etc
Library
system
Volumes
Looks like "/ " when accessing as user "Bob"
Looks like "/ " when accessing as user "Betty"
FTP share point incorporated within virtual root
Bob
Betty
Data
Photos
FTP server
FTP Root
FTP Root
Looks like "/ " to anonymous FTP users
FTP root
Data
Photos
Symbolic link

Users access FTP share points through symbolic links attached to the FTP Root directory. The symbolic links are created automatically when you create the FTP share points.

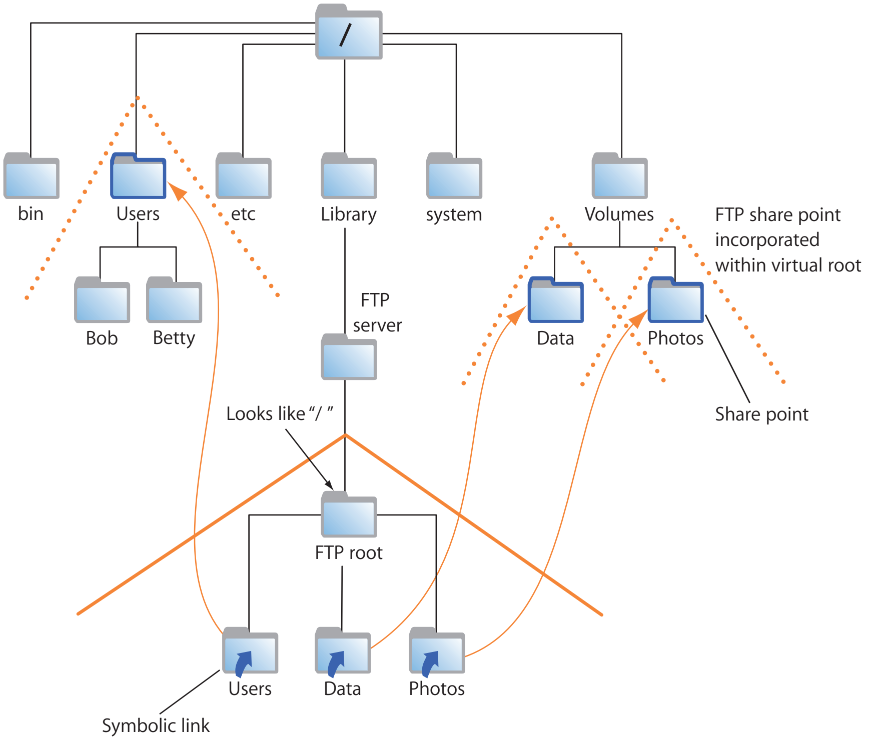
Note that in this example, /Users, /Volumes/Data, and /Volumes/Photos are FTP share points. All users can see the home directories of other users because they are subdirectories of the Users share point.

Important: Regardless of the user environment setting, anonymous users and users without home directories are always logged into the "FTP Root and Share Points" environment.

Home Directory With Share Points

When the user environment option is set to "Home Directory with Share Points," authenticated users log in to their home directories and have access to the FTP root by means of a symbolic link automatically created in their home directories. Users access other FTP share points through symbolic links in the FTP root. As always, access to the FTP share points is controlled by user access privileges.

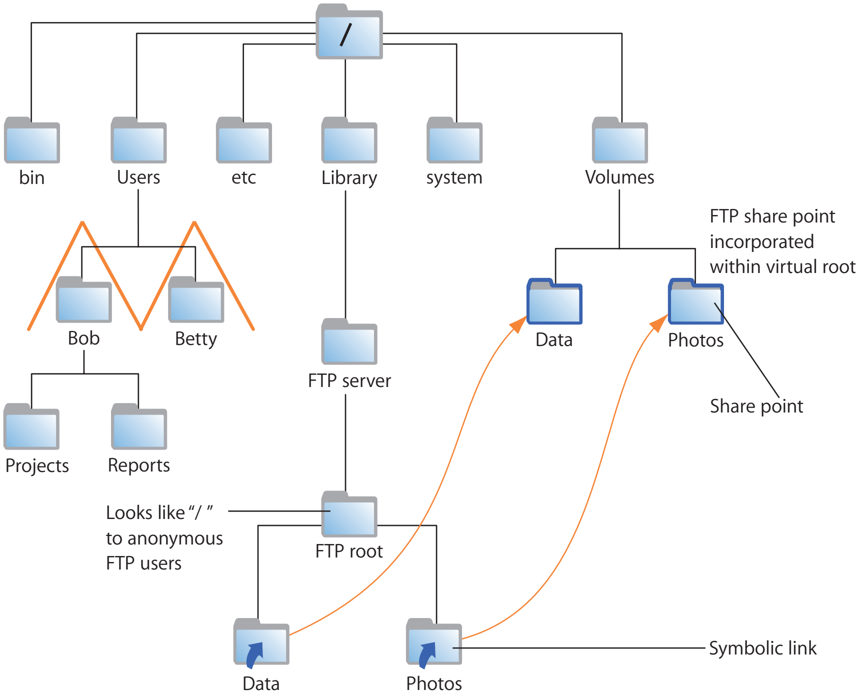
Note: For users to access their home directories, you must configure the share point in which the directories reside to be shared using FTP.



If you change the FTP root, the symbolic link in a user's home directory reflects that change. For example, if you change the FTP root to /Volumes/Extra/NewRoot, the symbolic link created in the user's home directory would be called NewRoot.

Home Directory Only

When you choose the Home Directory Only option, authenticated users are confined to their home directories and do not have access to the FTP root or other FTP share points, as shown in the following illustration.



Anonymous users and users without home directories still have access to the FTP root but cannot browse the FTP share points.

On-the-Fly File Conversion

FTP service in Mac OS X Server allows users to request compressed or decompressed versions of information on the server. A file-name suffix such as ".Z" or ".gz" indicates that the file is compressed. If a user requests a file called "Hamlet.txt" and the server only has a file named "Hamlet.txt.Z," it knows that the user wants the decompressed version, and delivers it to the user in that format.

In addition to standard file compression formats, FTP in Mac OS X Server has the ability to read files from either HFS or non-HFS volumes and convert the files to MacBinary (.bin) format. MacBinary is one of the most commonly used file compression formats for the Macintosh operating system.

The table below shows common file extensions and the type of compression they designate.

File extension	What it means
.gz	DEFLATE compression
.Z	UNIX compress
.bin	MacBinary encoding
.tar	UNIX tar archive
.tZ	UNIX compressed tar archive
.tar.Z	UNIX compressed tar archive
.crc	UNIX checksum file
.dmg	Mac OS X disk image

Files With Resource Forks

You can encourage Mac OS X clients to take advantage of on-the-fly conversion to help them transfer files created using older file systems that store information in resource forks. If you enable MacBinary and disk image auto-conversion in FTP service settings, files with resource forks will be listed as .bin files on the FTP clients. When a client asks to have one of these files transferred, on-the-fly conversion will recognize the .bin suffix and convert 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 the FTP service settings in Server Admin. See "Configuring General Settings" on page 83.

FTP service specifications

- Maximum number of connected users (the default setting is 50 for authenticated users and 50 for anonymous 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

Read "Before Setting Up FTP Service" on page 81 for issues you should keep in mind when you set up FTP service.

Step 2: Configure FTP General settings

The General settings let you display banner and welcome messages, set the number of login attempts, and provide an administrator email address. See "Configuring General Settings" on page 83.

Step 3: Configure FTP Messages settings

The Access settings let you specify the number of authenticated and anonymous users that can connect to the server. See "Changing the Greeting Messages" on page 84.

Step 4: Configure FTP Logging settings

The Logging settings let you specify the FTP-related events you want to log for authenticated and anonymous users. See "Choosing Logging Options" on page 84.

Step 5: Configure FTP Advanced settings

The Advanced settings let you change the FTP root and choose which items user can see. See "Changing Advanced Settings" on page 85.

Step 6: Create an "uploads" folder for anonymous users (optional)

If you enabled anonymous access in Step 2, you may want to create a folder for anonymous users to upload files. The folder must be named "uploads." It is not a share point, but must have appropriate access privileges. See "Creating an Uploads Folder for Anonymous Users" on page 85.

Step 7: Create share points and share them using FTP

Use the Sharing module of Workgroup Manager to specify the share points that you want to make available through FTP. You must explicitly configure a share point to use FTP in order for FTP users to be able to access the share point. See "Creating a Share Point" on page 33 and "Changing FTP Settings for a Share Point" on page 37.

Step 8: Start FTP service

After you have configured FTP, start the service to make it available. See "Starting FTP Service" on page 85.

Before Setting Up FTP Service

Consider the type of information you need to share and who your clients are when determining whether to offer FTP service. FTP works well when you want to transfer large files such as applications and databases. In addition, if you want to allow guest (anonymous) users to download files, FTP is a secure way to provide this service.

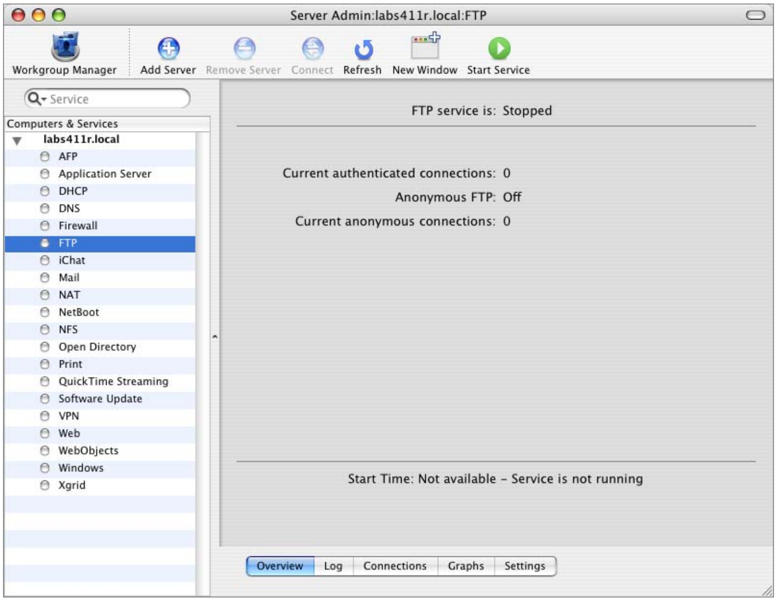
Server Security and Anonymous Users

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 you can keep information secure.

Anonymous FTP users are only allowed to upload files into a special folder named "uploads" in the FTP root. If the uploads folder doesn't exist, anonymous users will not be able to upload files at all.

To ensure the security of your FTP server, by default anonymous users cannot:

- Delete files
- Rename files
- Overwrite files
- Change permissions of files



FTP service is: Stopped

Current authenticated connections: 0
Anonymous FTP: Off
Current anonymous connections: 0

Start Time: Not available – Service is not running

Setting Up FTP Service

You use the Server Admin application to set up and enable FTP service. Changes you make to FTP service settings affect only new connections. Users who are currently connected will not see the changes.

Configuring General Settings

You can use the General settings to limit the number of login attempts, provide an administrator email address, and limit the number and type of users.

To configure the FTP General settings:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click General.
3. To change the number of times a user can try to connect before they are disconnected, type a number in "Disconnect after __ failed login attempts."
4. To provide a contact for your users, type an email address following "FTP administrator email address."
5. Under Access, choose a method from the Authentication pop-up menu.
6. Type a number in the "Allow a maximum of __ authenticated users" field to limit the number of authenticated users who can connect to your server at the same time.

   Authenticated users have accounts on the server. You can view or add them using the Accounts module of Workgroup Manager.
7. Select "Enable anonymous access" to allow anonymous users to connect to the server.

   Anonymous users can log in using the name "ftp" or "anonymous." They do not need a password to log in, but they will be prompted to enter their email addresses.

   Before selecting this option, you should review the privileges assigned to your share points carefully to make sure there are no security holes.
8. Type a number in the "Allow a maximum of __ anonymous users" field to limit the number of anonymous users who can connect to your server at the same time.
9. To have files with resource forks listed with a .bin suffix so that clients will take advantage of automatic file conversion when transferring them, select "Enable MacBinary and Disk Image auto-conversion."
10. Click Save.

From the Command Line

You can also change FTP service settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing the Greeting Messages

Users see the banner message when they first contact your server (before they log in) and the welcome message when they log in.

To change the banner and welcome messages:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Messages.
3. Edit the message text.
4. Select "Show banner message" and "Show welcome message."
5. Click Save.

From the Command Line

You can also change the FTP service banner message using the `serveradmin` command in Terminal or by editing the files /Library/FTPServer/Messages/banner.txt and /Library/FTPServer/Messages/welcome.txt. For more information, see the file services chapter of the command-line administration guide.

Choosing Logging Options

The Logging settings let you choose which FTP-related events to record.

For either authenticated or anonymous users, you can record:

- Uploads
- Downloads
- FTP commands
- Rule violation attempts

To configure the FTP Logging settings:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Logging.
3. In the "Log authenticated users" section, select events you want to record in the FTP log for authenticated users.
4. In the "Log anonymous users" section, select events you want to record in the FTP log for anonymous users.
5. Click Save.

To view the log, select FTP in Server Admin and click Log.

From the Command Line

You can also change the FTP service logging settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Advanced Settings

The Advanced settings let you specify the directories that FTP users can access.

You can change the FTP root directory and choose whether users see the FTP root and share points, home directories and share points, or home directories only.

To configure the FTP Advanced settings:

1 Open Server Admin and select FTP in the Computers & Services list.

2 Click Settings (near the bottom of the window), then click Advanced.

3 For "Authenticated users see," choose the type of user (chroot) environment you want to use: FTP Root and Share Points, Home Directory with Share Points, or Home Directory Only.

For more information, see "FTP Users" on page 76.

4 To change the FTP root, enter the pathname in the FTP Root field.

For more information, see "The FTP Root Directory" on page 76.

From the Command Line

You can also change the FTP service settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Creating an Uploads Folder for Anonymous Users

The uploads folder provides a place for anonymous users to upload files to the FTP server. It must exist at the top level of the FTP root directory and be named "uploads." (If you have changed the FTP root directory, then the uploads folder must be at the root of that directory.)

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's FTP root directory.

2 Set privileges for the folder to allow guest users to write to it.

From the Command Line

You can set up an FTP upload directory using the `mkdir` and `chmod` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Starting FTP Service

Start FTP file service to make the service available to your client users.

To start FTP service:

1 Open Server Admin and select FTP in the Computers & Services list.

2 Click Start Service (near the top of the window).

From the Command Line

You can also start the FTP service using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing FTP Service

This section describes how to perform typical day-to-day management tasks for FTP service once you have it up and running.

Stopping FTP Service

You stop FTP service using Server Admin.

Important: When you stop FTP service, users are disconnected without warning.

To stop FTP service:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Stop Service (near the top of the window).

From the Command Line

You can also stop the FTP service using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Allowing Anonymous User Access

You can allow guests to log in to your FTP server with the user name "ftp" or "anonymous." They don't need a password to log in, but they will be prompted to enter an email address.

For better security, do not enable anonymous access.

To allow anonymous FTP service:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click General.
3. Under Access, select "Enable anonymous access."
4. Click Save.

From the Command Line

You can also allow anonymous FTP access using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing the User Environment

You use the Advanced pane of Configure FTP Service to change the user environment.

To change the FTP user environment:

1 Open Server Admin and select FTP in the Computers & Services list.

2 Click Settings (near the bottom of the window), then click Advanced.

3 Choose the type of user environment you want to provide from the "Authenticated users see" pop-up menu.

"FTP Root and Share Points" sets up the Users directory as a share point. Authenticated users log in to their home directories, if they're available. Both authenticated and anonymous users can see other users' home directories.

"Home Directory with Share Points" logs authenticated FTP users in to their home directories. They have access to home directories, the FTP root, and FTP share points.

"Home Directory Only" restricts authenticated FTP to user home directories.

4 Click Save.

Regardless of the user environment you choose, access to all 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 directories (or whose home directories are not located in a share point to which they have access) are always logged in at the root level of the FTP environment.

Changing the FTP Root Directory

The Advanced settings allow you to change the path to the FTP root directory.

To specify a different FTP root:

1 If it doesn't already exist, create the directory you want to use and configure it as an FTP share point.

2 Open Server Admin and select FTP in the Computers & Services list.

3 Click Settings (near the bottom of the window), then click Advanced.

4 Type the path to the new directory in the "Authenticated user FTP root" field or click the Browse button next to the field and select it.

From the Command Line

You can also change the FTP service root directory using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing the Log

You use Server Admin to view the FTP log.

To view FTP log:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Log (near the bottom of the window).

To choose the types of events that are recorded, open Server Admin, select AFP, click Settings, then click Logging.

From the Command Line

You can also view the FTP log using the `cat` or `tail` commands in Terminal. For more information, see the file services chapter of the command-line administration guide.

Displaying 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 may not display the message in an obvious place, or they may 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 is displayed when a user first contacts the server, before they log in. The welcome message is displayed after they successfully log in.

To display banner and welcome messages to users:

1. Open Server Admin and select FTP in the Computers & Services list.
2. Click Settings (near the bottom of the window).
3. Click Messages.
4. Select "Show welcome message" and edit the text of the message.
5. Select "Show banner message," edit the text of the message, and click Save.

From the Command Line

You can also set the FTP service to display these messages using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Displaying Messages Using message.txt Files

If an FTP user opens a directory on your server that contains a file named "message.txt," the file contents are displayed as a message. The user sees the message only the first time he or she connects to the directory during an FTP session. You can use the message to notify users of important information or changes.

Using README Messages

If you place a file called README in a directory, an FTP user who opens that directory receives a message letting them know that the file exists and when it was last updated. Then the user can choose whether to open and read the file.

Solving Problems

6

This chapter lists possible solutions to common problems you might encounter while working with the file services in Mac OS X Server.

Problems are listed in the following categories:

- Problems with share points
- Problems with AFP service
- Problems with Windows service
- Problems with NFS service
- Problems with FTP service

Problems With Share Points

There are several ways to diagnose and solve problems with share points.

Users Can't Access a Shared Optical Media

- Make sure the optical media is a share point.
- If you share multiple media, make sure that each is shared using a unique name in the Sharing pane.

Can't Access External Volumes Using Server Admin or Workgroup Manager

- If a server is at the login window, the remote user of Server Admin (or Workgroup Manager) will not be able to manage external volumes such as FireWire drives. To solve this problem, make sure the server is logged in.

Users Can’t Find a Shared Item

- If a user can’t find a shared item, check the access privileges for the item. The user must have Read access privileges to the share point where the item is located and to each folder in the path to the item.
- Keep in mind that server administrators don’t see share points the same way a user does over AFP because administrators see everything on the server. To see share points from a user’s perspective, select “Enable administrator to masquerade as any registered user” in the Access pane of the Settings pane of the 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 the network services administration guide.

Users Can’t Open Their Home Directories

- Make sure the share point used for home directories is set up as a network mount for home directories in Workgroup Manager.
- Make sure the share point is created in the same Open Directory domain as your user accounts.
- Make sure the client computer is set to use the correct Open Directory domain using Directory Access.

Users Can’t Find a Volume or Directory to Use as a Share Point

- Make sure the volume or directory name does not contain a slash (“/”) character. Workgroup Manager’s Sharing window, which lists the volumes and directories on your server, does not correctly display the names of volumes and directories (folders) that include the slash (“/”) character.
- Make sure that you’re not using special characters in the name of the volume or directory.

Users Can’t See the Contents of a Share Point

If you set Write Only access privileges to a share point, users won’t be able to see its contents.

Problems With AFP Service

There are several ways to diagnose and solve AFP problems.

User 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 Apple file service. If you can’t connect to other network resources from the user’s computer, the network connection may not be working.
- Make sure the file server is running. You can use the Ping pane in Network Utility to check whether the server at the specified IP address can receive packets from clients over the network.

- If the user is searching for the server via AppleTalk (in the Chooser), make sure you've enabled browsing over AppleTalk in the General pane of the AFP service settings, and that AppleTalk is active on both the server and the user's computer.
- Check the name you assigned to the file server and make sure users are looking for the correct name.

User Can't Connect to the 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.
- Verify that logging in is enabled for the user in the Users & Groups module of Workgroup Manager.
- Check to see if the maximum number of client connections has been reached (in the Apple File Service Status window). If it has, other users should try to connect later.
- Make sure the server that stores users and groups is running.
- Verify that the user has AppleShare 3.7 or later installed on his or her computer. Administrators who want to use the admin password to log in as a user need at least AppleShare 3.7.
- Make sure IP filter service is configured to allow access on port 548 if the user is trying to connect to the server from a remote location. For more on IP filtering, see the network services administration guide.

User Doesn't See Login Greeting

- Upgrade the software on the user's computer. Apple file service client computers must be using AppleShare client software version 3.7 or later.

Problems With Windows Services

There are several ways to diagnose and solve SMB/CIFS problems.

User Can't See the Windows Server in the Network Neighborhood

- Make sure users' computers are properly configured for TCP/IP and have the appropriate Windows networking software installed.
- Enable guest access for Windows users.
- Go to the DOS prompt on the client computer and type `ping <IP address>`, where `<IP address>` is your server's address. If the ping fails, then there is a TCP/IP problem.
- If users' computers are on a different subnet from the server, you must have a WINS server on your network.

  Note: If Windows computers are properly configured for networking and connected to the network, client users can connect to the file server even if they can't see the server icon in the Network Neighborhood window.

User Can't Log in to the Windows Server

- If you're using Password Server to authenticate users, check to make sure that it is configured correctly.
- If you have user accounts created in a previous version of Mac OS X Server (version 10.1 or earlier) that are still configured to use Authentication Manager, make sure that Authentication Manager is enabled. Then reset the passwords of existing users who will be using Windows services. Reset the user's password and try again.

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 will cause errors on the client side.
- Incompatible versions of NFS can cause problems.
- NFS service supports only one world export per volume. This includes NetBoot share points.
- Use `showmount -e` *`IP address`*, where IP address is the server's address, to see the available NFS mounts.
- For information about using NFS to host home directories, see to the user management guide.

Problems With FTP Service

There are several ways to diagnose and solve FTP problems.

FTP Connections Are Refused

- Verify that the user is entering the correct DNS name or IP address for the server.
- Make sure FTP service is turned on.
- Make sure the user has appropriate access privileges to the shared volume.
- See if the maximum number of connections has been reached. To do this, open Server Admin, select FTP in the Computers & Services 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 configured correctly for TCP/IP. If there doesn't appear to be a problem with the TCP/IP settings, use a "pinging" utility to check network connections.
- See if there is a DNS problem by trying to connect using the IP address of the FTP server instead of its DNS name. If the connection works with the IP address, there may be a problem with the DNS server.
- Verify that the user is correctly entering his or her short name and typing the correct password. User names and passwords with special characters or double-byte characters will not work. To find the user's short name, double-click the user's name in the Users & Groups list.

- See if there are any problems with directory services, and if the directory services server is operating and connected to the network. For help with directory services, see the Open Directory administration guide.
- Verify that IP filter service is configured to allow access to the appropriate ports. If clients still can't connect, see if the client is using FTP passive mode and turn it off. Passive mode causes the FTP server to open a connection to the client on a dynamically determined port, which could conflict with port filters set up in IP filter service.
- Check the /Library/FTPServer/Messages/error.txt file for clues as to what the problem might be.

Clients Can't Connect to the FTP Server

- See if the client is using FTP passive mode, and turn it off. Passive mode causes the FTP server to open a connection on a dynamically determined port to the client, which could conflict with port filters set up in IP filter service.

Anonymous FTP Users Can't Connect

- Verify that anonymous access is turned on.
- See if the maximum number of anonymous user connections has been reached. To do this, open Server Admin and click FTP in the Computers & Services list.

Glossary

AFP Apple Filing Protocol. A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

access control A method of controlling which computers can access a network or network services.

access control list See **ACL**.

ACL Access Control List. A list maintained by a system that defines the rights of users and groups to access resources on the system.

address A number or other identifier that uniquely identifies a computer on a network, a block of data stored on a disk, or a location in a computer memory. See also **IP address**, **MAC address**.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined "admin" group.

alias Another email address at your domain that redirects incoming email to an existing user.

Apple Filing Protocol See **AFP**.

automount To make a share point appear automatically on a client computer. See also **mount**.

bit A single piece of information, with a value of either 0 or 1.

CIFS Common Internet File System. See **SMB/CIFS**.

client A computer (or a user of the computer) that requests data or services from another computer, or server.

command line The text you type at a shell prompt when using a command-line interface.

command-line interface A way of interfacing with the computer (for example, to run programs or modify file system permissions) by entering text commands at a shell prompt.

Common Internet File System See **SMB/CIFS**.

daemon A program that runs in the background and provides important system services, such as processing incoming email or handling requests from the network.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a lease period—the length of time the client computer may use the address.

directory Also known as a folder. A hierarchically organized list of files and/or other directories.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a directory node or simply a directory.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

DNS domain A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

DNS name A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a **domain name**.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

domain name See **DNS name**.

Domain Name System See **DNS**.

drop box A shared folder with privileges that allow other users to write to, but not read, the folder's contents. Only the owner has full access. Drop boxes should be created only using AFP. When a folder is shared using AFP, the ownership of an item written to the folder is automatically transferred to the owner of the folder, thus giving the owner of a drop box full access to and control over items put into it.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a website visitor.

export In the Network File System (NFS), a way of sharing a directory with clients on a network. TBD for RAID context.

file server A computer that serves files to clients. A file server may be a general-purpose computer that's capable of hosting additional applications or a computer capable only of serving files.

file system A scheme for storing data on storage devices that allows applications to read and write files without having to deal with lower-level details.

File Transfer Protocol See **FTP**.

FTP File Transfer Protocol. A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

guest user A user who can log in to your server without a user name or password.

home directory A folder for a user's personal use. Mac OS X also uses the home directory, for example, to store system preferences and managed user settings for Mac OS X users.

host Another name for a server.

host name A unique name for a server, historically referred to as the UNIX hostname. The Mac OS X Server host name is used primarily for client access to NFS home directories. A server determines its host name by using the first name available from the following sources: the name specified in the /etc/hostconfig file (HOSTNAME=some-host-name); the name provided by the DHCP or BootP server for the primary IP address; the first name returned by a reverse DNS (address-to-name) query for the primary IP address; the local hostname; the name "localhost."

Internet Generally speaking, a set of interconnected computer networks communicating through a common protocol (TCP/IP). The Internet (note the capitalization) is the most extensive publicly accessible system of interconnected computer networks in the world.

Internet Protocol See **IP**.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP address A unique numeric address that identifies a computer on the Internet.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

local hostname A name that designates a computer on a local subnet. It can be used without a global DNS system to resolve names to IP addresses. It consists of lowercase letters, numbers, or hyphens (except as the last characters), and ends with ".local" (e.g, bills-computer.local). Although the name is derived by default from the computer name, a user can specify this name in the Network pane of System Preferences. It can be changed easily, and can be used anywhere a DNS name or fully qualified domain name is used. It can only resolve on the same subnet as the computer using it.

logical disk A storage device that appears to a user as a single disk for storing files, even though it might actually consist of more than one physical disk drive. An Xsan volume, for example, is a logical disk that behaves like a single disk even though it consists of multiple storage pools that are, in turn, made up of multiple LUNs, each of which contains multiple physical disks.

Mac OS X The latest version of the Apple operating system. Mac OS X combines the reliability of UNIX with the ease of use of Macintosh.

Mac OS X Server An industrial-strength server platform that supports Mac, Windows, UNIX, and Linux clients out of the box and provides a suite of scalable workgroup and network services plus advanced remote management tools.

mount (verb) In general, to make a remote directory or volume available for access on a local system. In Xsan, to cause an Xsan volume to appear on a client's desktop, just like a local disk.

mulitcast DNS A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. This proposed Internet standard protocol is sometimes referred to as "ZeroConf." For more information, visit www.apple.com or www.zeroconf.org. To see how this protocol is used in Mac OS X Server, see **local hostname**.

Network File System See **NFS**.

network interface Your computer's hardware connection to a network. This includes (but isn't limited to) Ethernet connections, AirPort cards, and FireWire connections.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

nfsd daemon An NFS server process that runs continuously behind the scenes and processes read and write requests from clients. The more daemons that are available, the more concurrent clients can be served.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, NetInfo, or Active Directory protocols; BSD configuration files; and network services.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

oplocks See **opportunistic locking**.

opportunistic locking Also known as oplocks. A feature of Windows services that prevents users of shared files from changing the same file at the same time. Opportunistic locking locks the file or part of the file for exclusive use, but also caches the user's changes locally on the client computer for improved performance.

owner The owner of an item can change access permissions to the item. The owner may also change the group entry to any group in which the owner is a member. By default the owner has Read & Write permissions.

password An alphanumeric string used to authenticate the identity of a user or to authorize access to files or services.

pathname The location of an item within a file system, represented as a series of names separated by slashes (/).

permissions Settings that define the kind of access users have to shared items in a file system. You can assign four types of permissions to a share point, folder, or file: read/write, read-only, write-only, and none (no access). See also **privileges**.

port A sort of virtual mail slot. A server uses port numbers to determine which application should receive data packets. Firewalls use port numbers to determine whether data packets are allowed to traverse a local network. "Port" usually refers to either a TCP or UDP port.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

process A program that has started executing and has a portion of memory allocated to it.

protocol A set of rules that determines how data is sent back and forth between two applications.

QTSS QuickTime Streaming Server. A technology that lets you deliver media over the Internet in real time.

QuickTime A set of Macintosh system extensions or a Windows dynamic-link library that supports the composition and playing of movies.

QuickTime Streaming Server See **QTSS**.

Samba Open source software that provides file, print, authentication, authorization, name resolution, and network service browsing to Windows clients using the SMB/CIFS protocol.

server A computer that provides services (such as file service, mail service, or web service) to other computers or network devices.

Server Message Block/Common Internet File System See **SMB/CIFS**.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

short name An abbreviated name for a user. The short name is used by Mac OS X for home directories, authentication, and email addresses.

single sign-on An authentication strategy that relieves users from entering a name and password separately for every network service. Mac OS X Server uses Kerberos to enable single sign-on.

SLP DA Service Location Protocol Directory Agent. A protocol that registers services available on a network and gives users easy access to them. When a service is added to the network, the service uses SLP to register itself on the network. SLP/DA uses a centralized repository for registered network services.

SMB/CIFS Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB/CIFS to provide access to servers, printers, and other network resources.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

ticket, Kerberos A temporary credential that proves a Kerberos client's identity to a service.

Transmission Control Protocol See **TCP**.

UDP User Datagram Protocol. A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

UID User ID. A number that uniquely identifies a user within a file system. Mac OS X computers use the UID to keep track of a user's directory and file ownership.

URL Uniform Resource Locator. The address of a computer, file, or resource that can be accessed on a local network or the Internet. The URL is made up of the name of the protocol needed to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

User Datagram Protocol See **UDP**.

user ID See **UID**.

user name The long name for a user, sometimes referred to as the user's "real" name. See also **short name**.

volume A mountable allocation of storage that behaves, from the client's perspective, like a local hard disk, hard disk partition, or network volume. In Xsan, a volume consists of one or more storage pools. See also **logical disk**.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

WINS Windows Internet Naming Service. A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

Index