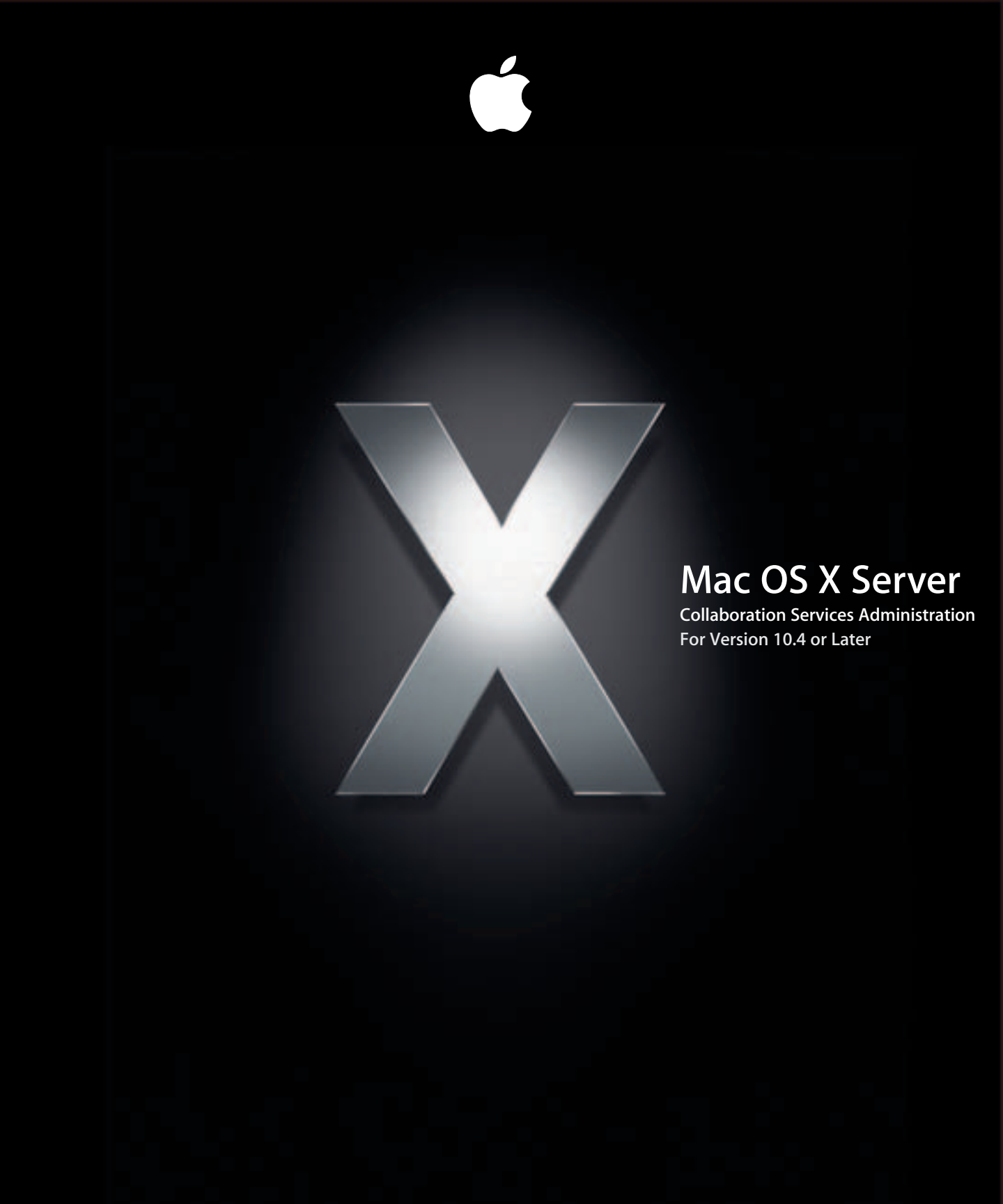


Mac OS X Server

Collaboration Services Administration

For Version 10.4 or Later

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

019-0744/07-21-06

Contents

About This Guide

This guide describes the collaboration services you can set up using Mac OS X Server.

Collaboration services promote interactions among users, facilitating teamwork and productivity. This guide highlights the advantages and usage of collaboration services and tells you how to implement them.

What's New in Version 10.4

Mac OS X Server continues to provide such collaborative support as mailing list management, group account and folder management, and cross-platform file sharing. Two new collaborative services have been added for version 10.4:

- **Weblog service.** Mac OS X Server provides a multiuser weblog server that complies with the RSS and Atom XML standards. Weblog service supports Open Directory authentication. For additional safety, users can access Weblog service using a website that's SSL enabled.
- **iChat service.** Mac OS X Server provides instant messaging for Macintosh, Windows, and Linux users. User authentication is integrated into Open Directory, and setup and administration of iChat service is done using the graphical Server Admin application.

What's in This Guide

This guide includes the following chapters:

- Chapter 1, "Collaboration in Action," introduces the collaboration services and describes several scenarios in which they're useful.
- Chapter 2, "Weblog Service," describes how to set up, manage, and use a Weblog server so that users the server supports can share information by blogging.
- Chapter 3, "iChat Service," describes how to set up, manage, and use an iChat server so that users the server supports can communicate by chatting.
- Chapter 4, "File Sharing Services," summarizes features of the five file-sharing protocols, and it tells you where to find detailed information for setting up and managing them.

- Chapter 5, "Group Accounts," describes how group accounts and managed preferences facilitate collaboration, and it tells you where to find detailed administration information.
- Chapter 6, "Mail Services," summarizes mail service, mailing lists, and WebMail features, and it and tells you where to find detailed administration information.
- The "Glossary" defines terms you'll encounter as you read this guide.

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

Using Onscreen Help

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, 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:
Getting Started, Getting Started Supplement, and *Mac OS X Server Worksheet*	Install Mac OS X Server and set it up for the first time.
Collaboration Services Administration	Set up and manage weblog, chat, and other services that facilitate interactions among users.
Command-line Administration	Use commands and configuration files to perform server administration tasks in a UNIX command shell.
Deploying Mac OS X Computers for K-12 Education	Configure and deploy Mac OS X Server and a set of Mac OS X computers for use by K-12 staff, teachers, and students.
Deploying Mac OS X Server for High Performance Computing	Set up and manage Mac OS X Server and Apple cluster computers to speed up processing of complex computations.
File Services Administration	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB/CIFS.
High Availability Administration	Manage IP failover, link aggregation, load balancing, and other hardware and software configurations to ensure high availability of Mac OS X Server services.
Java Application Server Guide	Configure and administer a JBoss application server on Mac OS X Server.
Mac OS X Security Configuration	Secure Mac OS X client computers.
Mac OS X Server Security Configuration	Secure Mac OS X Server computers.
Mail Service Administration	Set up, configure, and administer mail services on the server.
Migrating to Mac OS X Server From Windows NT	Move accounts, shared folders, and services from Windows NT servers to Mac OS X Server.
Network Services Administration	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.
Open Directory Administration	Manage directory and authentication services.
Print Service Administration	Host shared printers and manage their associated queues and print jobs.
QuickTime Streaming Server 5.5 Administration	Set up and manage QuickTime streaming services.
System Imaging and Software Update Administration	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.

This guide ...	tells you how to:
Upgrading And Migrating	Use data and service settings that are currently being used on earlier versions of the server software.
User Management	Create and manage user accounts, groups, and computer lists. Set up managed preferences for Mac OS X clients.

Getting Documentation Updates

Periodically, Apple posts new onscreen help topics, revised guides, and 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 (www.apple.com/macosx/server/)—gateway to extensive product and technology information.

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

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

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

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

Collaboration in Action

1

Mac OS X Server's collaboration services help users communicate and share information.

Organizations of all sizes benefit from collaboration services. They offer a wide variety of interaction techniques:

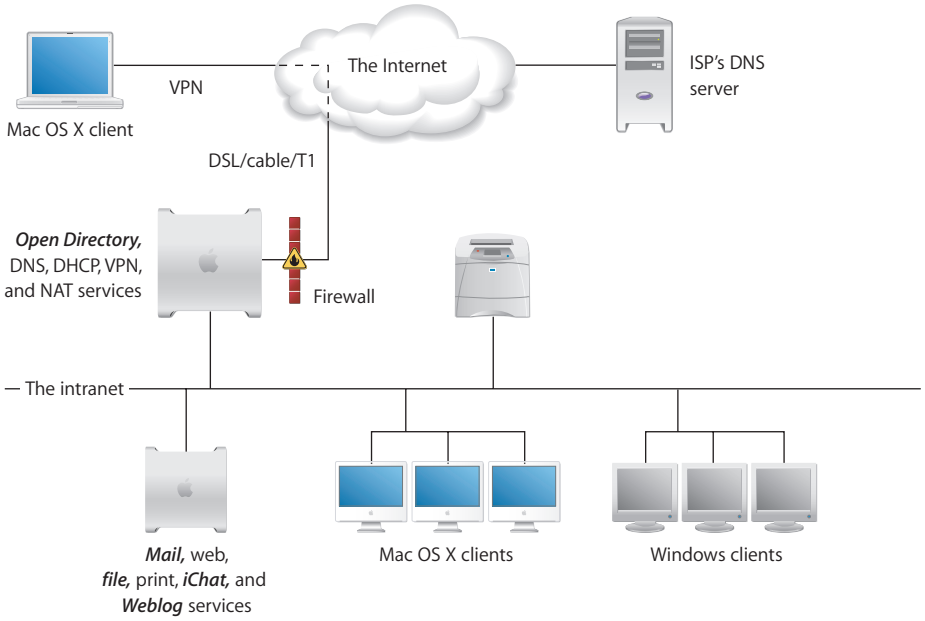
- **Weblog service** provides a simple way to publish and publicize information using webpages.
- **iChat service** provides secure instant messaging for the users a server supports.
- **File sharing services** provide controlled, secure access to folders and files from different kinds of client computers.
- **Group accounts** offer a way to customize the work environment to support groups of users.
- **Mail services** facilitate collaboration among users who use mail applications.

This chapter takes a brief look at how these services might be deployed in small- to medium-sized organizations and in large organizations. Subsequent chapters focus on individual items in the list above.

Collaboration Services in Small- to Medium-Sized Organizations

Small businesses (fewer than 100 employees) and medium businesses (about 100-500 employees) typically hire an Internet Service Provider (ISP) to provide Domain Name System (DNS) and DSL (digital subscriber line) services for a company intranet. The typical company intranet uses one to four servers.

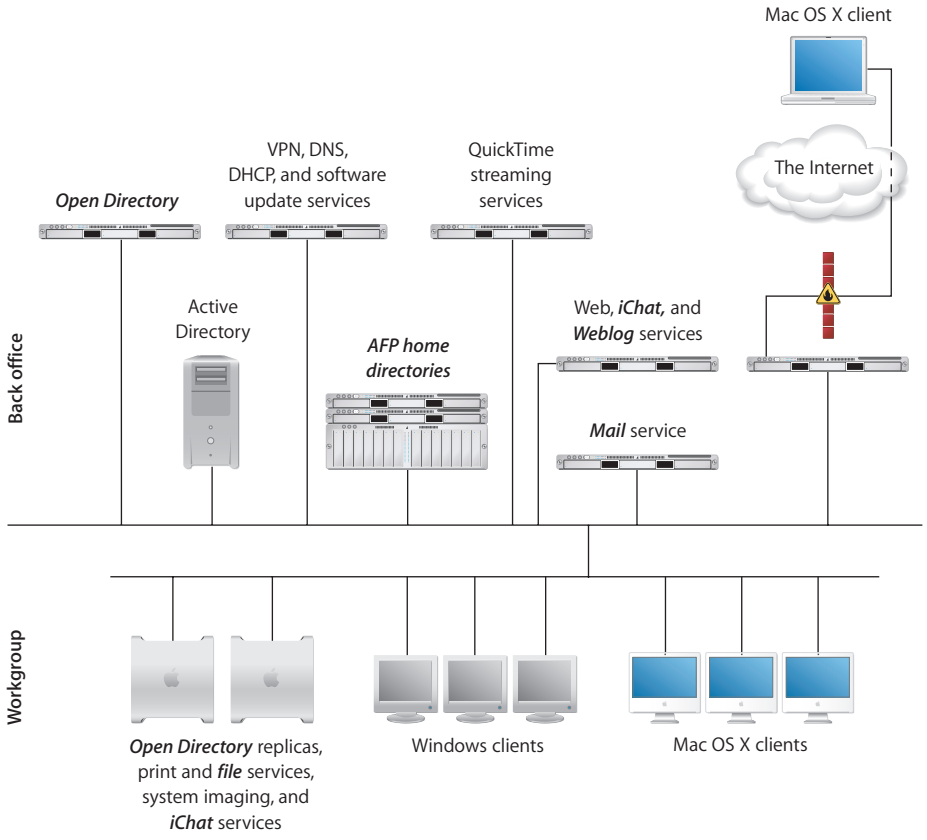
The following scenario has three servers: one behind the firewall hosting directory and network services, another behind the firewall hosting collaboration services, and a third outside the firewall hosting iChat service.



- The firewall between the server and the Internet protects the intranet from unauthorized access.
- An Open Directory master LDAP directory on one server provides user and group authentication support.
- DHCP service provides dynamic IP addresses to intranet client computers. The server and printer have static addresses, but client computers have dynamic addresses.
- The ISP's DNS service provides a DNS domain name (example.com) for the company. DNS service provided by Mac OS X Server provides name services for the server, the printer, and any other intranet device that has a static IP address.
- NAT service lets intranet users share the ISP's IP address for Internet access, while VPN lets employees access their company intranet securely over the Internet when they're working away from the office.
- The iChat server inside the firewall hosts instant messages among authorized users.

Collaboration Services in Large Organizations

In large organizations, collaboration services are usually deployed at both corporate and workgroup levels.



- Open Directory services are deployed on a back-office server, then replicated in workgroups. That way, directory data can be managed centrally, but distributed geographically.
- Other back-office servers are devoted to specific company-wide needs, such as network services, mail services, and web, iChat, and Weblog services.
- Home directories for company employees are stored centrally and configured for access using AFP (Apple Filing Protocol) service.

  AFP service takes advantage of a cost-effective configuration of two Xserves and an Xserve RAID.

Weblog Service

2

Weblog service provides a simple way to publish and publicize information using webpages.

Blogging, the practice of using a webpage as an electronic journal or newsletter, has become a popular way to exchange information among users with common interests.

The webpage, referred to as a *weblog* or a *blog,* is used to post entries and display them in chronological order. *Entries* are usually short articles, focused on a particular topic. Because they're web-based, entries can include electronic links, which make viewing related content fast and easy.

How Weblogs Promote Collaboration

In a business or education setting, weblogs offer a way to exchange information in an ongoing, organized, and focused way. Using weblog entries to monitor information as it becomes available is much easier than trying to keep track of long sequences of email messages:

- Project team members can post weekly status summaries on a weblog, creating a week-by-week view of a project's progress.
- Members of a product development team can conduct discussions, post design ideas, and exchange comments.
- Human resources departments can use a weblog to disseminate health plan and other benefit information. New employees can access past information, but existing employees can view only new entries as they're posted.
- In an educational scenario, weblogs offer a way to track the results of experiments over time. They can also be used to publish campus holiday and activity schedules, assignments, even cafeteria menus.

Weblog entries can be posted and changed only by weblog owners. But weblogs promote interactions among users who read them by supporting comments and trackbacks:

- A *comment* is used by weblog users to post a response to an entry. The response is visible to anyone else who reads the entry.
- A *trackback*, which is an electronic link between two entries, lets a weblog author (or blogger) respond or refer to another blogger's entry by using an entry on his or her own weblog.

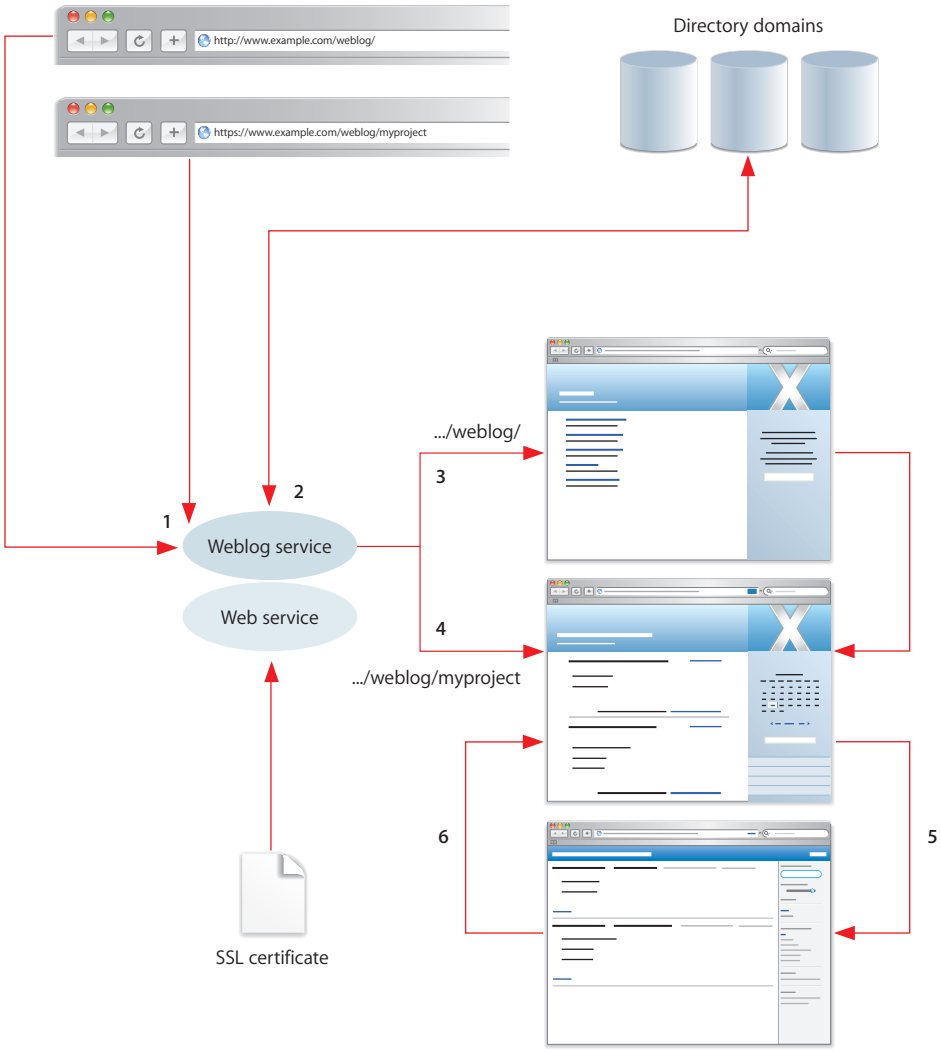
  To create a trackback, a blogger posts the entry on his or her weblog and includes in it a link to the other blogger's entry. When you read the other blogger's entry, the contents of the entry that created the trackback is visible, as is a link back to the weblog where that entry resides.

Weblog visibility is also promoted by a complementary standard called *Really Simple Syndication* (RSS). When weblogs support the RSS format, they generate RSS feeds that are discoverable by RSS aggregators, applications that search, format, and display RSS feeds. Users simply click a link in the RSS aggregator to view the original entry. RSS aggregators make finding weblogs and staying abreast of new entries easy. Mac OS X computer users can use Safari to monitor weblogs, because Safari has a built-in RSS aggregator.

Weblog Service in Action

Mac OS X Server's Weblog service provides a way for the users and groups a server supports to interact using weblogs. Each server can host one weblog for each user and group defined in directories in the server's Open Directory search path.

Easy to set up once you've started web service, Weblog service uses Open Directory authentication and, if enabled, web service's SSL to safeguard weblog usage.



1 To view or create a weblog, you access Weblog service by typing a URL in a web browser, such as Safari.

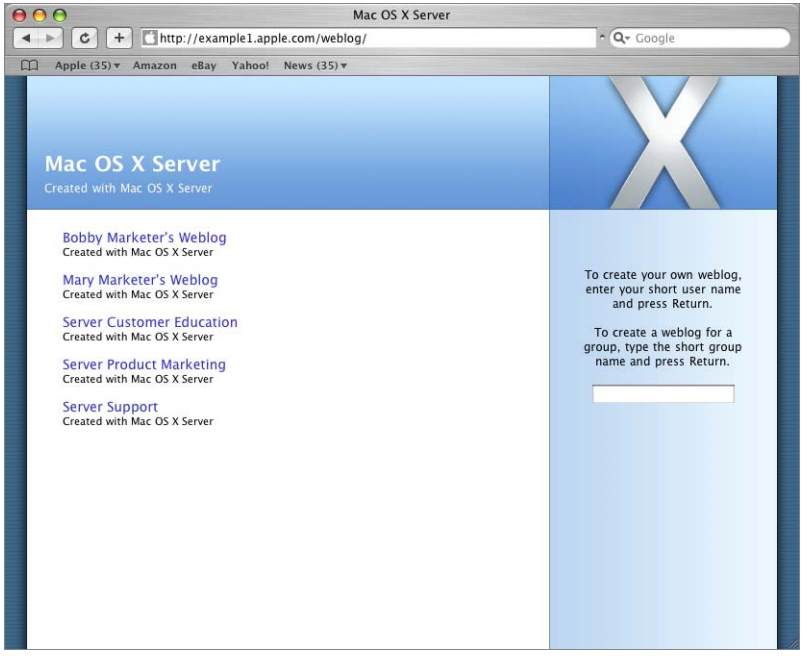
In the picture above, the URL that starts with "http://" displays a page that lets you create a weblog or access weblogs that already exist.

The other URL starts with "https://" to illustrate what you'd type if www.example.com were a site that's SSL enabled. This URL also shows how to access a specific weblog, in this case a weblog that belongs to a group named "myproject."

2 Weblog service authenticates users by using Open Directory authentication. You can be authenticated only if the user name and password you enter when prompted match those for a user defined in a directory domain in the server's Open Directory search path.

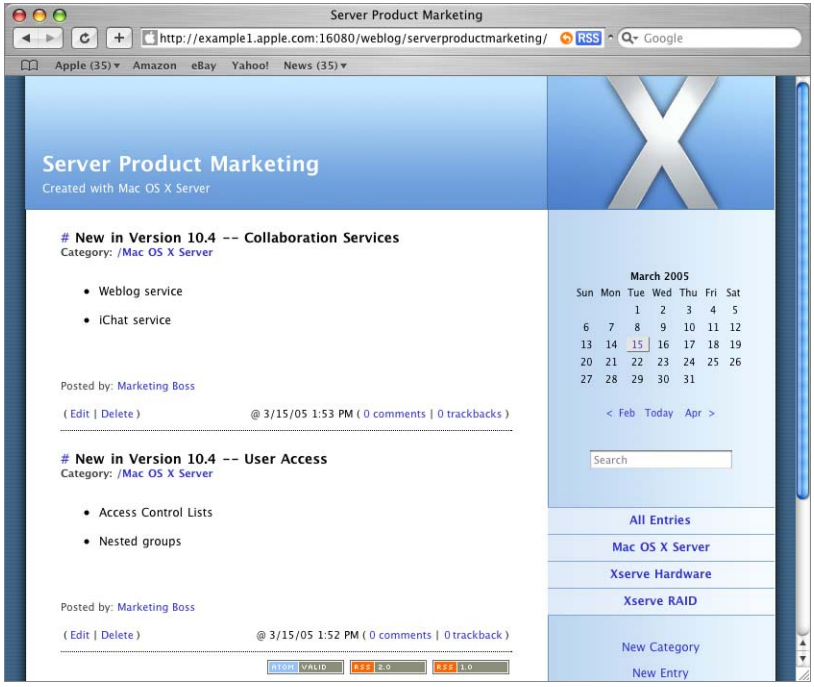
Weblog service also checks to make sure you're authorized to use Weblog service. The server administrator can optionally deny specific users access to Weblog service.

3 When you've submitted a URL ending in "/Weblog/", the Weblog service front page appears.



On this page, you can create a weblog for yourself or you can create one for a group to which you belong. You can also access an existing weblog by clicking one of the links on the page.

4 When viewing a weblog that isn't yours or associated with a group to which you belong, you can read entries, view associated comments and trackbacks, and add comments. If the weblog owner has grouped entries by categories or subcategories, click one to view entries on a particular topic, such as Mac OS X Server in this example. To view entries posted on a particular day, click the day in the calendar.

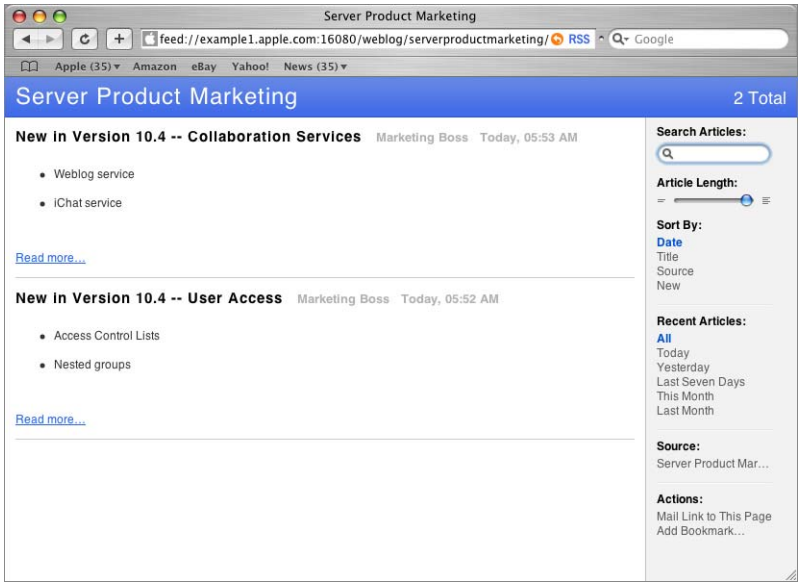


If a weblog belongs to you, or to a group to which you belong, you can create and organize entries and change other aspects of the weblog by using the Settings link. For example, you can let only specific users view your weblog. And you can change the appearance of your weblog by choosing different themes.

5 When you want to monitor the entries on a weblog, you can subscribe to the weblog's RSS feed. All Weblog service's weblogs automatically generate RSS feeds.

To subscribe to a weblog's feed in Safari, you'd simply click the RSS icon in the address field when the weblog is displayed. You can bookmark the RSS feed and place it in a location that's convenient for you to access.

6 When you're ready to monitor a weblog, use your RSS bookmark to list information about and links to entries in the weblog.



The remainder of this chapter tells you how to administer Weblog service and use the weblogs it hosts.

Setting Up Weblog Service for the First Time

You activate weblogging by starting web service in Server Admin, then establishing a few default weblog settings. You can set up one Weblog server per server computer.

To set up Weblog service for the first time:

1 Open Server Admin.

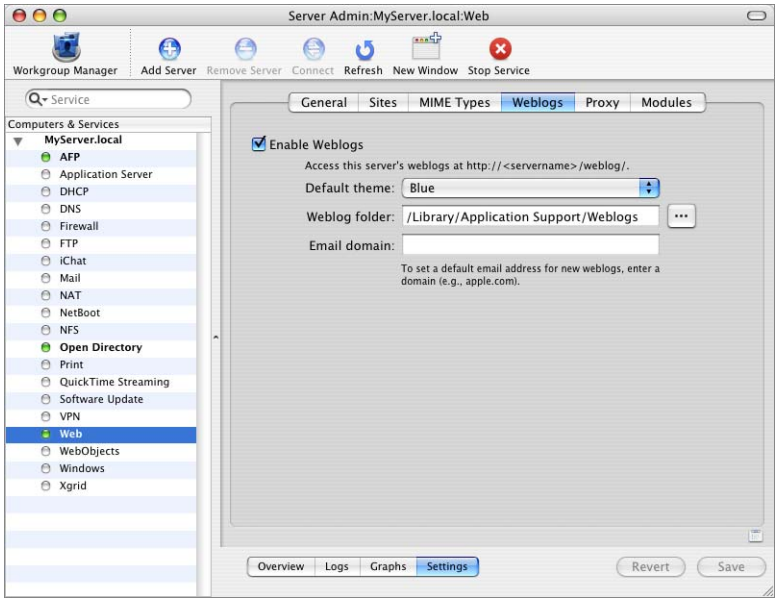
2 If the server on which you want Weblog service to run isn't listed in the Computers & Services list, click Connect to connect with the server.

3 Select the server in the list, and then click Web.

4 If web service isn't running, click Start Service.

To maximize the security of user interactions with the server hosting weblogs, have users access weblogs through a site that has Secure Sockets Layer (SSL) enabled. Follow the instructions in the web technologies administration guide for how to set up websites and configure them to use SSL. SSL works in conjunction with a digital certificate that provides a certified identity for the server by establishing a secure, encrypted exchange of information.

5 Click Settings, click Weblogs, and select Enable Weblogs. This setting enables weblog access through any website that web service is configured to support.



6 Choose a default theme.

A theme controls the appearance of a weblog. Themes determine the color, size, location, and other attributes of weblog elements. Each theme is implemented using a style sheet, as "Understanding Weblog Service Configuration Files" on page 23 describes.

The default theme is used when a weblog is initially created, but weblog owners can change the theme any time. The default theme also controls the appearance of Weblog service's front page.

7 Identify a weblog folder, used to store weblog files.

By default, weblog files are stored in /Library/Application Support/Weblogs/ on the computer hosting Weblog service. You can click Browse to select a different folder, such as a folder on a RAID device or on another computer.

See "Understanding Weblog Files" on page 24 for more information about weblog file storage.

8 Optionally, specify a default email domain, such as "example.com."

The email domain is used to construct an initial email address for a weblog. For example, a user whose short name is "john" would have an email address of john@example.com displayed on his weblog initially, but the user can change it.

9 Click Save.

10 Make sure that the Weblog server's Open Directory search path includes directories in which users and group members you want to support with Weblog service are defined. The Open Directory administration guide explains how to set up search paths.

Any user or group member defined in the Open Directory search path is now authorized to create and access weblogs on the server unless you deny them access to Weblog service as described in "Defining Who Can Create Weblogs" on page 22.

Managing Weblog Service

This section describes tasks server administrators use to manage Weblog service.

Defining Who Can Create Weblogs

You control who can create weblogs by using Open Directory authentication and Weblog service access settings. If you want a user to be able to create weblogs:

- Make sure the user is a user or member of a group that's defined in the Open Directory search path of the Weblog server.
- Also make sure the user has Weblog service access. To grant and deny Weblog service access, open Server Admin, select the Weblog server in the Computers & Services list, click Settings, then click Access.

Defining Who Can View Weblogs

Users who own a weblog or belong to a group that owns a weblog control who can view it by using Reader settings in the weblog. See "Controlling Who Can View Weblogs" on page 26 for instructions.

Using SSL for Weblog Access

To maximize the security of user interactions with the server hosting weblogs, have users access weblogs through a site that has Secure Sockets Layer (SSL) enabled.

When SSL is implemented on a server, a browser connects to it using the "https" prefix in the URL rather than "http." The "s" indicates that the server is secure.

The web technologies administration guide describes how to set up sites and enable them to use SSL.

Changing Weblog Service Settings

You use Server Admin to change Weblog service settings.

To make changes to Weblog service settings:

1. Open Server Admin, select the server in the Computers & Services list, click Web in the list beneath the server, then click Weblogs.
2. To disable or enable Weblog service, use the Enable Weblogs checkbox.
3. If you change the default theme, all new weblogs initially use the new theme you select.
4. If you change the weblog folder, existing folders and files within it are not automatically moved, and Weblog service automatically restarts when you save your changes.

   If you want to continue using any existing weblog folders and files, you need to manually move them to the new weblog folder location. "Understanding Weblog Files" on page 24 identifies what to move.
5. If you change the default email domain, all new weblogs initially use the new one.
6. Click Save when you're finished making changes.

Understanding Weblog Service Configuration Files

Files that define Weblog service properties are stored in:

/Library/Tomcat/blojsom_root/webapps/blojsom/

Configuration files are grouped into subfolders. Many of them contain settings for Blojsom, the open-source project on which the Weblog service is based. Two subfolders are Apple-specific:

- A folder named Stylesheets contains style sheets, or themes. They have the extension .css, which stands for Cascading Style Sheet.

  CSS is a standard for specifying the appearance of text and other elements in webpages and other sources.

  All the stylesheets in this folder are listed in the "Default theme" popup menu for weblog settings in Server Admin and in the dialog box associated with the Settings link on individual weblogs.
- Configuration files for each weblog are in a folder called WEB-INF. This folder contains subfolders named using short user or group names. The subfolders contain various files, including one named blog.properties, which stores the weblog settings that weblog owners can change using the Settings link in their weblogs.

Understanding Weblog Files

User and group weblog files are stored in the weblog folder set using Server Admin. By default, it's the following folder on the computer hosting Weblog service:

/Library/Application Support/weblogs/

Files for each weblog are stored in the weblog folder:

- Each user and group weblog has its own folder just beneath the weblog folder, named using the short name of the user or group.
- Within each weblog folder is a folder for each category or subcategory.
- Within each category folder are two files for each entry. A file with the extension .txt contains the content, and a file with the extension .meta contains comments and identifies the entry's author.

If you change the identity of the top weblog folder in Server Admin, existing folders and files are not automatically moved.

Weblog File Maintenance

You may want to archive folders and files when users or groups are deleted from the directories the server supports.

Understanding Weblog Service Logs

Weblog service logs are stored in:

/Library/Tomcat/blojsom_root/webapps/blojsom/logs

Using Weblogs

This section describes various ways for users to work with individual weblogs.

Creating Weblogs

If you satisfy the conditions in "Defining Who Can Create Weblogs" on page 22, you can create a weblog.

To create a weblog:

1. Open Safari or another popular web browser such as Mozilla, Firefox, or Internet Explorer.
2. In the address field, type http://*domain-name*/weblog/ where *domain-name* identifies the web server (www.example.com).

   If the web server has an SSL-enabled site, for maximum security specify that site in the address and use the https prefix in the URL. Type https://*domain-name*/weblog/ where *domain-name* identifies the site with SSL enabled.
3. The webpage that appears lists links to all weblogs that have already been created on the server and lets you create a new weblog.

To create your own weblog, enter your short user name and press Return. If your short name is the same as the short name of a group in the server's Open Directory search path, Weblog service assumes you've entered a user name.

To create a weblog for use by members of a group, type the short group name and press Return.

4 The new weblog appears, reflecting the default Weblog service settings defined in Server Admin.

5 Now you can customize the weblog settings or perform other activities. First, click Login to authenticate.

Click Settings to change weblog setting values.

Click New Category to create a category within which to group new entries.

Click New Entry to create a new entry. See "Creating a New Entry" on page 27 for instructions.

6 Optionally, click Logout when you're finished making changes. Weblog service automatically logs out users after 30 minutes of inactivity.

To access the weblog later, type http://*domain-name*/weblog/*short-name* or https://*domain-name*/weblog/*short-name*, where *domain-name* identifies the web server (www.example.com) and *short-name* is the short name of a user or group.

Accessing Weblogs

You use a web browser to access a weblog.

To access a weblog:

1 Open Safari or another popular web browser such as Mozilla, Firefox, or Internet Explorer.

2 To access a particular weblog, in the address field type http://*domain-name*/weblog/*short-name*, where *domain-name* identifies the web server (www.example.com), and *short-name* is the short name of the user or group that owns the weblog.

If the web server has an SSL-enabled site, for maximium security specify that site in the address and use the https URL prefix. Type https://*domain-name*/weblog/*short-name,* where *domain-name* identifies the site with SSL enabled.

3 To select a weblog from a list of weblogs on the server, simply type http://*domain-name*/weblog/ or https://*domain-name*/weblog/. The webpage that appears is the Weblog service's front page, which provides links to all the weblogs it hosts. When you see the weblog you want to access, click its link.

Controlling Who Can View Weblogs

Users or members of a group who own a weblog control who can view the weblog.

To control access to a weblog:

1. Access a weblog you're authorized to change. See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. Click Settings.
4. Use the Readers field to specify who you want to be able to view your weblog.

   To let anyone read your weblog, leave the field blank.

   To let only specific users or groups defined in the Weblog server's search path read your weblog, enter their short names, one per line.

Viewing Weblog Entries

When you first open a weblog, the most recent 20 entries are visible, the latest at the top of the list.

There are several ways to filter a weblog's entries for viewing:

- To view entries made on a particular day, click the day highlighted on the calendar.
- To view all entries, click All Entries.
- To view entries in a particular category, click the category. If a category has subcategories, click one to view only its entries.
- To view entries whose content contains a particular string, type the string in the Search field and press Return.

Customizing Weblog Settings

Weblog settings control some of the text that's displayed on the weblog and can be used to limit who can access the weblog.

To change weblog settings:

1. Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. Click Settings.
4. Change settings as desired to modify information that's displayed on the weblog.
5. Click Save.

Creating a New Category

You can define categories and subcategories that group weblog entries. Categorizing entries makes it easier for others to view entries about a particular subject.

Each category or subcategory you create becomes a folder in which related entries are stored. See "Understanding Weblog Files" on page 24 for more information.

To create a weblog category or subcategory:

1. Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. Click New Category.
4. From the Parent pop-up list, choose the item under which you want the category to be listed.
5. Type a name for the category.
6. Click Save.

Deleting a Category

When you delete a category or subcategory, any entries currently associated with it are moved to All Categories.

To delete a weblog category or subcategory:

1. Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. Select the category or subcategory you want to delete.
4. Click Delete Category.
5. Click OK.

Creating a New Entry

When you add a new entry to a weblog, you can optionally add it to a category you've defined.

To create a new entry:

1. Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. Click New Entry.
4. Optionally choose a category, then enter a title.

5 If you want the entry to create a trackback to someone else's entry, copy the trackback URL from that entry and paste it into the Trackback URL field.

To obtain the trackback URL for an entry hosted by Weblog service, access the entry and click the trackback link at the bottom of it. Copy the "Trackback URL for this entry," which was created by Weblog service when the entry was first created.

6 Type the entry contents in the box.

You can optionally embed these HTML tags in your content: a, b, blockquote, br, code, dd, dl, div, em, h1, h2, h3, h4, h5, h6, i, img, ol, lik, p, pre, span, strong, sub, sup, table, td, th, tr, u, and ul. Commonly used tags are:

Tag	Use	Example
b or strong	Make text boldface	text text
i or em	Make text italicized	text text
ul and li	Created a bulleted list	 - one - two
sub	Create a subscript	_i
sup	Create a superscript	²
img	Display a graphical image	

When you type a URL (http://www.example.com), a link is automatically generated for you.

7 Click Save.

The new entry identifies the author and displays the creation time.

Deleting an Entry

When you delete an entry, all files for the entry are deleted (see "Understanding Weblog Files" on page 24).

To delete an entry:

1 Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.

2 Click Login to authenticate.

3 In the entry you want to delete, click Delete.

Changing an Entry

You can change an entry's title, trackback URL, and content, but you can't change its category or time of creation.

To edit an entry:

1. Access a weblog you're authorized to change (you must be its owner or belong to a group that owns it). See "Accessing Weblogs" on page 25 for instructions.
2. Click Login to authenticate.
3. In the entry you want to edit, click Edit and make changes.
4. Click Save.

Using Comments

Users who can view weblogs can create comments for any of the entries.

To work with comments:

1. Access a weblog.
2. Display the entries of interest.
3. To view or create comments for an entry, click its Comments link. Existing comments are listed and you can optionally add a comment.
4. To add a comment, at a minimum identify yourself in the Author field and type your comment in the Comment field. Then click Submit Comment.

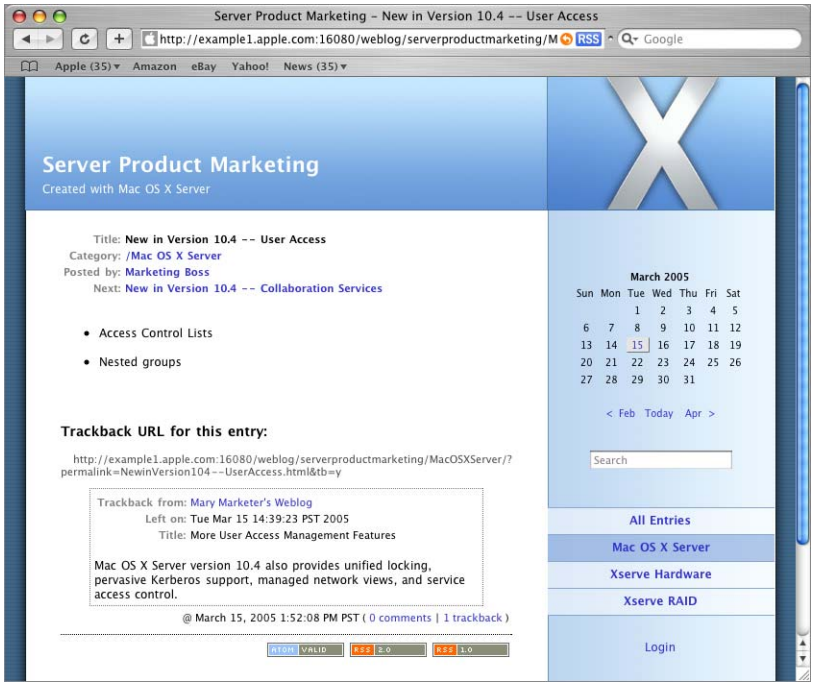
   Optionally, include your email address or a URL to related information.

Using Trackbacks

A trackback is a way for a blogger to respond or refer to another blogger's entry by using an entry on his or her own weblog.

To create a trackback, you post an entry on your weblog and include in it a link to the other blogger's entry. "Creating a New Entry" on page 27 describes how to associate a trackback link with an entry.

When you read the other blogger's entry and click its Trackback link, the contents of the entry that created the trackback is visible, as is a link back to the weblog where that entry resides. If other entries have created trackback links to the entry, they, too, are listed.



Using RSS to Subscribe to Weblogs

Weblogs created by Mac OS X Server's Weblog server automatically generate RSS feeds. Using Safari or an RSS aggregator application, you can subscribe to RSS feeds of interest to you.

To subscribe to weblogs using RSS in Safari:

1. Open Safari.
2. To track all weblogs on a server that you have access to, display Weblog service's front page.

   To track a particular weblog you have access to, display the weblog.

   "Accessing Weblogs" on page 25 tells you how.
3. Click the RSS icon in the Safari address field.

4 Bookmark the RSS feed.

If you want to monitor multiple weblogs, you can create a Bookmark Folder in Safari and add bookmarks for weblogs of interest to the folder.

See Safari help for information about how to use RSS feeds and bookmarks.

For Additional Information

Here are several resources that provide information related to Weblog service:

- The web technologies administration guide describes how to set up and manage web service.
- The Open Directory administration guide describes how to set up an Open Directory search path for the server hosting Weblog service.
- The website wiki.blojsom.com/wiki/ provides documentation about the open-source blog package on which Weblog service is based.
- There are several excellent books about weblogging. Search for them on websites such as www.oreilly.com/catalog/.

iChat Service

3

iChat service provides secure instant messaging for users Mac OS X Server supports.

Instant messaging comprises live interactions conducted between users by exchanging text, pictures, even audio and video on their computers. Instant messaging is usually referred to as *chatting,* because of its spontaneous, conversation-like qualities.

How Chatting Promotes Collaboration

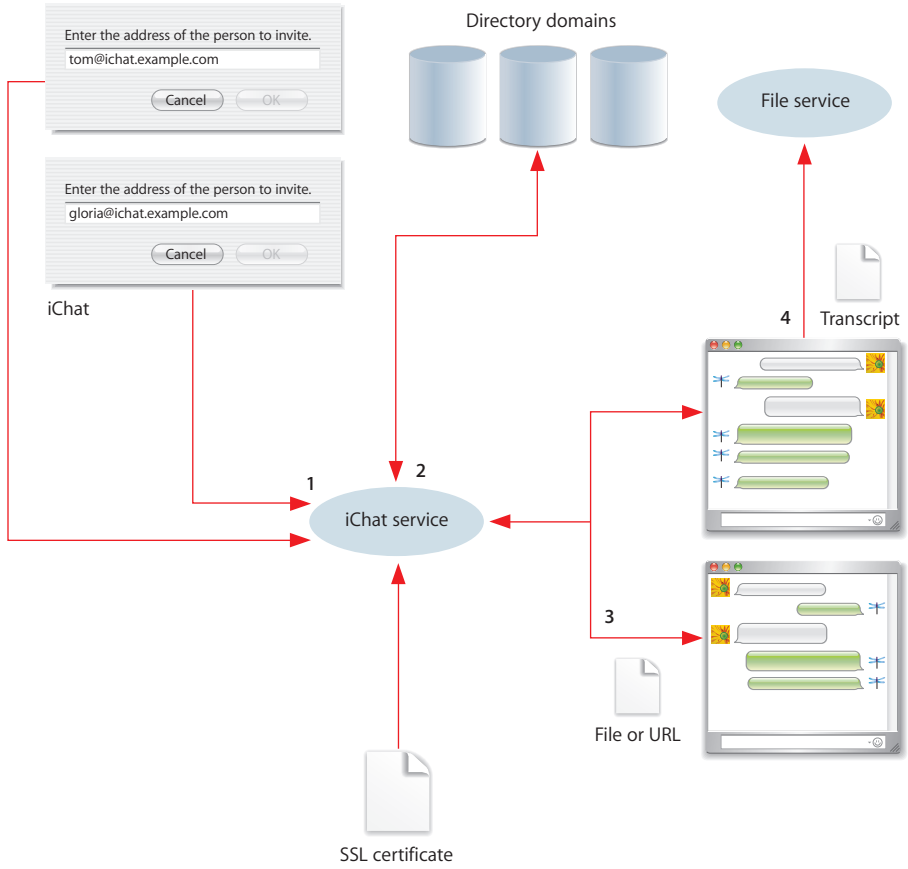
Chatting offers a way to collaborate without the delays of such solutions as email and weblogs or the expense of such approaches as using the telephone or holding meetings:

- Project team members can brainstorm solutions to issues, make plans, report progress, exchange pictures of designs.
- While chatting, you can exchange links to webpages or files to use as real-time references or for followup viewing.
- Text transcripts of chats can be made automatically when you want a written record of interactions without the distraction of taking notes.
- Weekly staff or project meetings can be conducted using chatting. And when staff or project team members are geographically dispersed, chatting offers an excellent replacement for meetings or conference calls.
- Instead of using text, you can chat using audio, taking advantage of microphones built into computers.
- If computers of chatters are equipped with a video camera, they can see *and* hear each other while chatting. Videoconferencing offers an extremely direct, personal, and engaging form of collaboration.

iChat Service in Action

Mac OS X Server's iChat service provides a secure way for users and groups that a server supports to interact using chatting.

In order to use iChat service on a particular server, users must be defined in directories the server uses to authenticate users. In addition, iChat service uses SSL to protect the privacy of users while they chat.



1 To start a chat with another user, you just need to know the user's short name and a domain name iChat service is configured to use.

In the picture above, the Tom and Gloria start a chat with each other using iChat service on ichat.example.com.

2 iChat service verifies the identity of Tom and Gloria by using Open Directory authentication. You can be authenticated only if you're defined in a directory domain in the server's Open Directory search path.

iChat service also makes sure that Tom and Gloria are authorized to use it. The server administrator can optionally deny access to the service to specific users.

3 Tom and Gloria can send files and URLs back and forth, making it easy to jointly review information.

4 Optionally, a transcript of the chat can be recorded and saved for use later.

The remainder of this chapter tells you how to administer and use iChat service.

Setting Up iChat Service for the First Time

You configure and activate iChat service using Server Admin.

To set up iChat service for the first time:

1 Open Server Admin.

2 If the server on which you want iChat service to run isn't listed in the Computers & Services list, click Connect to connect with the server.

3 Select the server in the list.

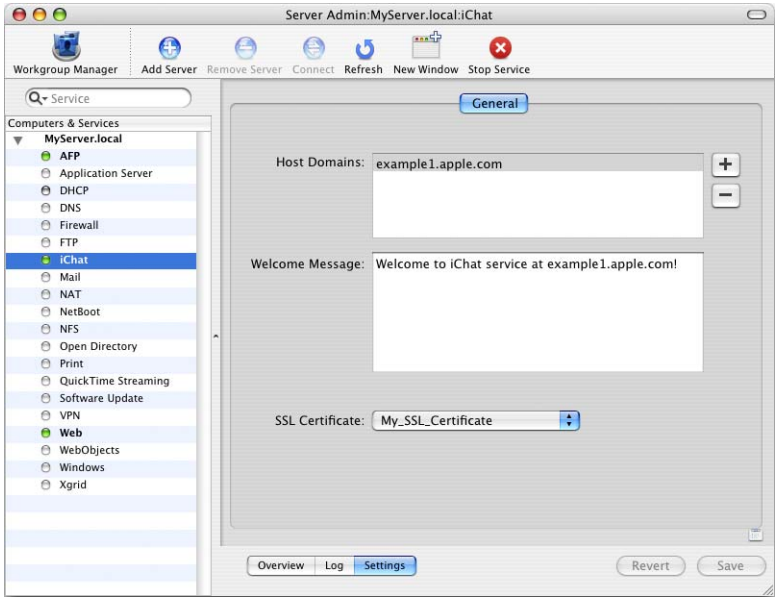
4 Make sure that the port iChat service uses is enabled.

Click Firewall under the selected server, and make sure that firewall service is running.

Click Settings, then click Services. Choose the address group of interest from the pop-up menu. Any traffic from addresses in the selected group can access iChat service if the first radio button is selected. If the second radio button is selected, make sure that there's a checkmark in the Allow column for iChat service.

See the network services administration guide for detailed information about firewall service and its settings.

5 Click iChat under the selected server in the Computers & Services list, then click Settings.



6 The Host Domains field designates the domain name(s) you want iChat service to support. Initially, the server's host name is displayed. You can add other names that resolve to the iChat server's IP address, such as aliases defined in DNS.

Host domains are used to construct screen names, which identify iChat service users. An example of a screen name is nancy@example1.apple.com.

7 The text in the Welcome Message window is displayed by chat clients when they connect with iChat service. Change the default text displayed in the field if you like.

8 From the SSL Certificate pop-up menu, choose a Secure Sockets Layer (SSL) certificate you want iChat service to use. The menu lists all SSL certificates that have been installed on the server. You can also choose Custom Configuration from the pop-up menu then click the Edit icon to import a different certificate.

See the mail service administration guide for complete information about defining, obtaining, and installing certificates on your server.

9 Click Save, and then click Start Service.

10 Make sure that the iChat server's Open Directory search path includes directories in which the users and group members that you want to communicate using iChat service are defined. The Open Directory administration guide explains how to set up search paths.

Any user or group member defined in the Open Directory search path is now authorized to use iChat service on the server unless you deny them access to iChat service, as described in "Defining iChat Service Access" on page 37.

Managing iChat Service

This section describes tasks server administrators use to manage iChat service.

Defining iChat Service Access

You control who can use iChat service by using Open Directory authentication and iChat service access settings. If you want a user to be able to use iChat service:

- Make sure the user is a user or member of a group that's defined in the Open Directory search path of the iChat server.
- Also make sure the user has iChat service access. To grant and deny iChat service access, open Server Admin, select the iChat server in the Computers & Services list, click Settings, then click Access.

Using SSL for iChat Service

To maximize the privacy of chats, iChat service uses SSL. SSL uses a digital certificate to certify the identity of the server and establish secure, encrypted data exchange.

You can use a self-signed certificate or a certificate imported from a Certificate Authority. See the mail service administration guide for complete information about defining, obtaining, and installing certificates on your server.

You identify an SSL certificate for iChat service to use the first time you set up iChat service, but you can use a different certificate later if you like.

To identify an SSL certificate for iChat service to use:

1. Open Server Admin, select the server in the Computers & Services list, click iChat in the list beneath the server, then click Settings.
2. From the SSL Certificate pop-up menu, choose the certificate you want iChat service to use. The menu lists all SSL certificates that have been installed on the server. To use a certificate not listed, select Custom Configuration from the pop-up menu.
3. Click Save.

Changing iChat Service Settings

You use Server Admin to change iChat service settings.

To make changes to iChat service settings:

1. Open Server Admin, select the server in the Computers & Services list, click iChat in the list beneath the server, then click Settings.
2. To disable or enable iChat service, click Stop Service or Start Service, respectively.
3. Change login or SSL information as required.
4. Click Save when you're finished making changes.

Understanding iChat Service Configuration File

iChat service configuration settings are stored in:

/etc/jabber/jabber.xml

The file includes settings for the Jabber/XMPP protocol. Jabber/XMPP is the open-source protocol used by the jabberd project to provide communication with clients running on a variety of different operating systems. iChat service supports the Jabber/XMPP protocol.

Understanding iChat Service Logs

The iChat service log is /var/log/system.log.

To view the iChat service log:

1. Open Server Admin.
2. Select the iChat server in the Computers & Services list.
3. Click iChat in the list beneath the server.
4. Click Log.

Using iChat Service

This section provides information that affects chat application users.

Before You Use iChat Service

To use iChat service running on a particular server to chat with another user:

- You must be defined in the Open Directory search path of that server.
- You must be authorized to use iChat service on that server.

You can chat only with users defined in the Open Directory search path of that server who are authorized to use its iChat service.

See "Defining iChat Service Access" on page 37 for more information about search paths and iChat service authorization.

Understanding iChat Service Screen Names

To use iChat service, you'll need a screen name. You'll also need to know the screen names of everyone you want to chat with using iChat service.

The iChat service screen name has the general format *user-short-name@iChat-domain-name* (nancy@ichat.example.com).The *user-short-name* is the short name of a user defined in the Open Directory search path of the server hosting iChat service. The *iChat-domain-name* identifies the server hosting iChat service.

Using iChat

To use iChat for chatting with other iChat service users, you need to set up an iChat service account. You do so by adding a Jabber account in iChat.

You can create the account when you first run iChat and enter initial setup information. You can also create the account after initial iChat setup by using the iChat > Preferences pane in iChat. See iChat help for instructions.

Since all buddy lists are saved on the server, they're available anytime and from anywhere you start an iChat service session.

Using Other Vendors' Chat Applications

iChat service supports instant messaging applications on Windows, Linux, and popular Personal Digital Assistants (PDAs) that support the Jabber protocol.

For Additional Information

Here are several resources that provide information related to iChat service:

- The network services administration guide describes how to set up and manage firewalls on the server hosting iChat service.
- The Open Directory administration guide describes how to set up an Open Directory search path for the server hosting iChat service.
- The mail service administration guide describes how to use SSL certificates.
- iChat help describes how to set up and use this Mac OS X chat application.
- The website jabberd.jabberstudio.org provides information about the open-source project that uses the Jabber/XMPP protocol, a protocol that iChat service supports.

File Sharing Services

4

File sharing services provide controlled, secure access to folders and files from different kinds of client computers.

Mac OS X Server's cross-platform file sharing services help groups work more efficiently by letting them share resources, archive projects, exchange and back up important documents, and conduct other file-focused activities.

How File Sharing Promotes Collaboration

In most organizations, files stored in a network-accessible folder are the primary way to store and share information:

- Sharing fonts, application preferences, pictures, and other resources lets you customize and unify group work environments.

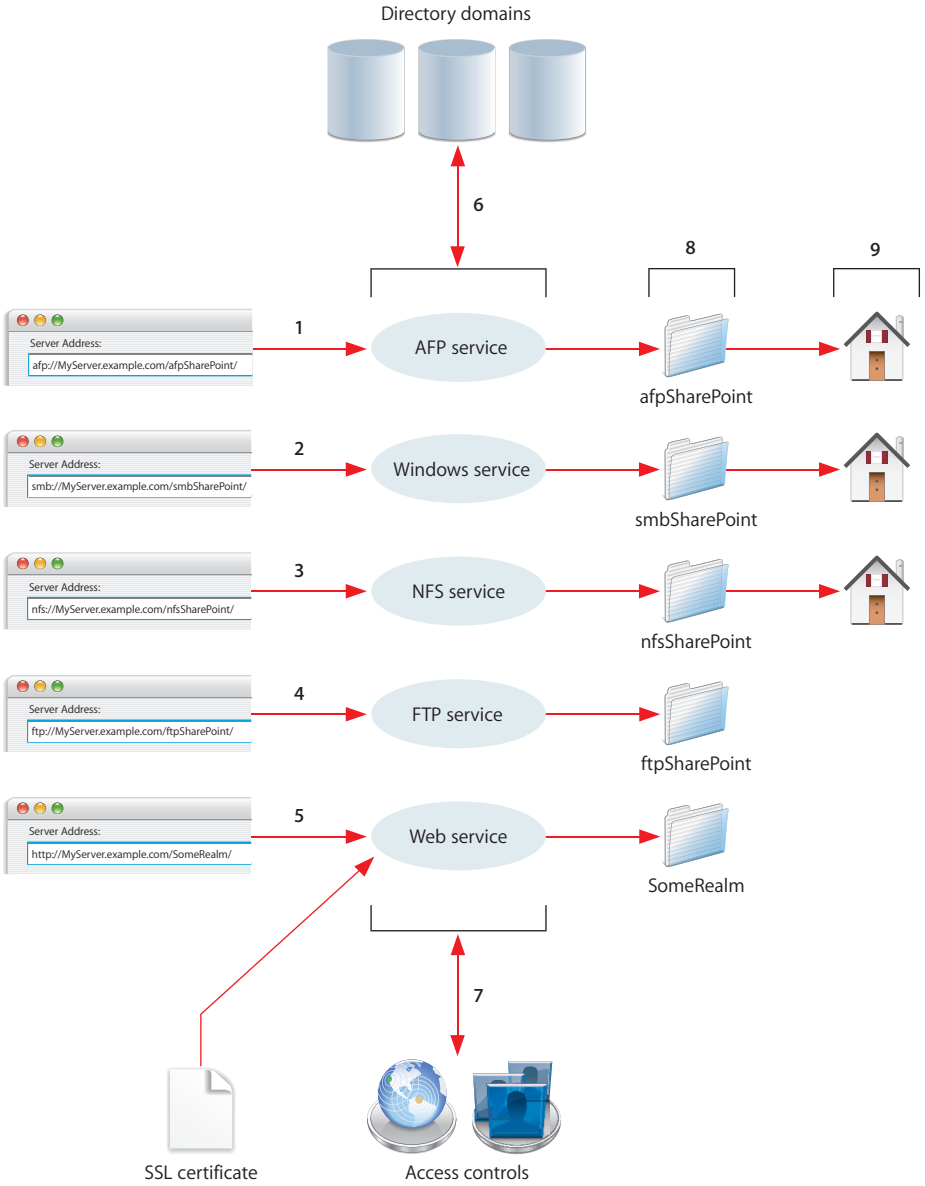
  For example, hosting a network-visible Library folder on Mac OS X Server makes it easy to distribute and update resources such as fonts, ColorSync profiles, application preferences, and templates across an entire workgroup. Mac OS X client computers automatically scan the contents of the Library folder, and system resources in the folder are instantly available to users.

- Sharing applications simplifies keeping them up to date. When you keep a site-licensed copy current, network users always have access to the latest version.
- Configuring access to folders and files lets you support the workflow of a group of users.

  For example, you can give writers and editors full access to documents, but limit reviewer access to read only.

File Sharing Services in Action

Mac OS X Server supports five protocols for accessing folders and files, all of which take advantage of Open Directory authentication. To further safeguard access, you can use several authorization techniques.



1 Apple File Service, which uses the Apple Filing Protocol (AFP), lets you share files among Macintosh clients.

2 Windows service uses the Server Message Block/Common Internet File System (SMB/CIFS) protocol to let you share files with clients who use Microsoft Windows 95, 98, ME, XP, NT 4.0, and 2000. Windows users can see shared folders using the My Network Places window (Windows XP and 2000) or the Network Neighborhood window (Windows 95, 98, or ME).

3 Network File System (NFS) service lets you share files with UNIX and Linux computer users.

4 File Transfer Protocol (FTP) service lets you share files using applications that support FTP. Many browsers, such as Microsoft Internet Explorer, accept an FTP address and display folders and files in the browser window.

5 Web-based Distributed Authoring and Versioning (WebDAV) lets you use a web server as a file server. Users of WebDAV-enabled applications (such as Macromedia Dreamweaver and Microsoft Office) can access WebDAV folders directly from those applications. You can safeguard WebDAV access using SSL if web service is configured to use an SSL certificate.

6 All file access services except NFS service authenticate users by using Open Directory authentication. Only users defined in a directory domain in the server's Open Directory search path can access files.

   Although NFS doesn't support name/password authentication, you can reshare NFS mounts using AFP, SMB/CIFS, or FTP, so that NFS users can be authenticated using Open Directory.

7 You configure additional access control settings using Server Admin and Workgroup Manager. These settings authorize users to access folders and files.

   Share point settings let you configure access permissions, which determine who can read files, change them, or perform other actions on them. Share points, used by all file access protocols, are points of access at the top level of a group of shared items.

   To make share points easy to find, you can configure them to automatically mount on a user's computer at login.

   Other authorization options are also available. For example, AFP and SBM/CIFS protocols support access control lists (ACLs). ACLs give you a way to craft share point, folder, and file access permissions with a high degree of precision. A wide range of permissions, including the right to modify access permissions, the right to create and delete or change files, the right to read permissions, and others, can be assigned to individual users and to groups, which can be nested. In addition, you can use inheritance to propagate permissions through a file system hierarchy.

   Access authorization is also available at the service level. AFP, SMB/CIFS, and FTP services can be set up to deny any access to specific users.

8 A user that meets authentication and authorization criteria can access folders and files within the target share point.

9 You can use an AFP, SMB/CIFS, or NFS share point to store network home directories. Network home directories give users access to their personal files from different computers and locations.

The following table contrasts the five file access protocols, and subsequent sections briefly focus on each protocol.

	AFP	SMB/CIFS	NFS	FTP	WebDAV
Open Directory authentication	x Kerberos supported	x	x if volumes are reshared using AFP, SMB/CIFS, or FTP	x Kerberos supported	x
Share point setup using Workgroup Manager	x	x	x	x	x
Service settings in Server Admin	x	x	x	x	x in web service
SSL					x if web service uses SSL
ACLs	x	x			
Service access control	x	x		x	
Network home directories	x	x	x		

Using AFP to Share Files

AFP allows Macintosh client users to connect to the server and access folders and files as if they were located on the user's own computer.

AFP offers:

- File sharing support for Macintosh clients over TCP/IP
- Autoreconnect support when a file server connection is interrupted
- Encrypted file sharing (AFP through SSH)
- Automatic creation of user home directories
- Kerberos v5 authentication for Mac OS X version 10.2 and later clients
- Fine-grain access controls for managing client connections and guest access
- Automatic disconnect of idle clients
- IPv6 support for AFP clients and server
- ACLs

AFP also lets you reshare NFS mounts using AFP. This feature provides a way for clients who are not on the local network to access NFS volumes via a secure, authenticated AFP connection.

Using SMB/CIFS to Share Files

Windows file service in Mac OS X Server allows Windows clients to connect to the server using SMB/CIFS over TCP/IP.

When you enable Windows file service, you can also enable several additional native Windows services:

- Windows Internet Naming Service (WINS), which allows clients across multiple subnets to perform name/address resolution
- Browsing, which allows clients to browse for available servers across subnets

You can set up (and replicate) Primary Domain Controller (PDC) services, which:

- Provide Windows domain authentication from the Windows login window
- Support Windows roaming profiles on Mac OS X Server

Mac OS X Server provides unified file locking across AFP and SMB/CIFS protocols, letting Windows users share files with users on other computers without conflict or corruption. SMB/CIFS also supports ACLs.

Using NFS to Share Files

NFS is the protocol used for file services on UNIX computers.

The NFS term for sharing is *export*. 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.

NFS does not support name/password authentication. It relies on client IP addresses to authenticate users and on client enforcement of permissions, not a secure approach in most networks. Therefore use NFS only if you are on a local area network (LAN) with trusted client computers, or if you are in an environment that can't use Apple file sharing or Windows file sharing. If you have Internet access and plan to export to World, your server should be behind a firewall.

You can reshare NFS mounts using AFP, Windows, and FTP so that users can access NFS volumes in a more restricted fashion.

Using FTP to Share Files

FTP allows computers to transfer files over the Internet. Clients using any operating system that supports FTP can connect to your FTP file server and download files, depending on the permissions you set. Most Internet browsers and a number of freeware applications can be used to access your FTP server.

FTP service in Mac OS X Server supports Kerberos v5 authentication and, for most FTP clients, resumption of interrupted FTP file transfers. Mac OS X Server also supports dynamic file conversion, allowing users to request compressed or decompressed versions of information on the server.

Mac OS X Server supports anonymous FTP and by default prevents anonymous FTP users from deleting files, renaming files, overwriting files, and changing file permissions. Explicit action must be taken by the server administrator to allow uploads from anonymous FTP users, and then only into a specific share point.

Using WebDAV to Share Files

Mac OS X Server supports WebDAV Internet file sharing as part of the built-in Apache web server and Mac OS X Server's web services.

Originally designed for collaborative web publishing, this enhancement to the HTTP protocol turns a website into a document database, enabling collaborative creation, editing, and searching from remote locations. With WebDAV enabled, any authorized WebDAV client, on any platform, can open files, make changes or additions, and save those revisions back to the web server. And because it uses HTTP (port 80), WebDAV can support file sharing through firewalls that don't allow FTP sharing.

For Additional Information

Several administration guides tell you how to set up and manage file services and home directories:

- The file services administration guide covers AFP, SMB/CIFS, FTP, and NFS services.
- The web technologies administration guide covers WebDAV.
- The user management guide covers home directories.
- The Windows administration guide provides additional information on sharing files with Windows users and on setting up SBM/CIFS share points for Windows user home directories.

Group Accounts

5

Group accounts offer a way to customize the work environment to support the needs of groups of users.

Mac OS X Server group accounts provide a way to manage and support groups of users, including their work environment attributes and access rights to folders, files, and computers.

How Groups Promote Collaboration

Groups offer several ways to promote the efficiency of users who belong to them and protect the privacy of group information:

- When you set up a group account, you can associate a server-resident group folder with the group. The group folder is a place for group members to exchange ideas and information. The group folder is easily created, and can be quickly configured to automatically mount or appear in the Dock when a group member logs in.
- You can set up other shared folders on the server for use by one or more groups.

  For example, you can add all English teachers to a group and give the group access to folders that store curriculum plans and student records. Teachers also might want to use shared folders to give students access to applications, handouts, and activity schedules, and to collect assignments.
- Group work environments can be customized by using managed preferences. *Managed preferences* are settings that control a user's computer experience. A group that has preferences managed is called a *workgroup*.

  For example, you can set up Dock and Finder preferences to dramatically simplify the work environment of lower-grade students. Or you can define Media Access preferences to prevent students from burning CDs or DVDs.
- If a user belongs to more than one workgroup, a list of the workgroups appears after login. The user selects a workgroup, and the environment defined using managed group preferences is set up. By logging in using different workgroups, users can move among environments that complement the needs of the moment.

For example, a marketing workgroup can enjoy an environment that promotes sharing information and applications for producing marketing materials. A New Employees workgroup can facilitate access to benefits information for recently hired employees.

- When you want to influence all members of a group at a global level but manage a subset of group members at a more focused level, you can nest groups.

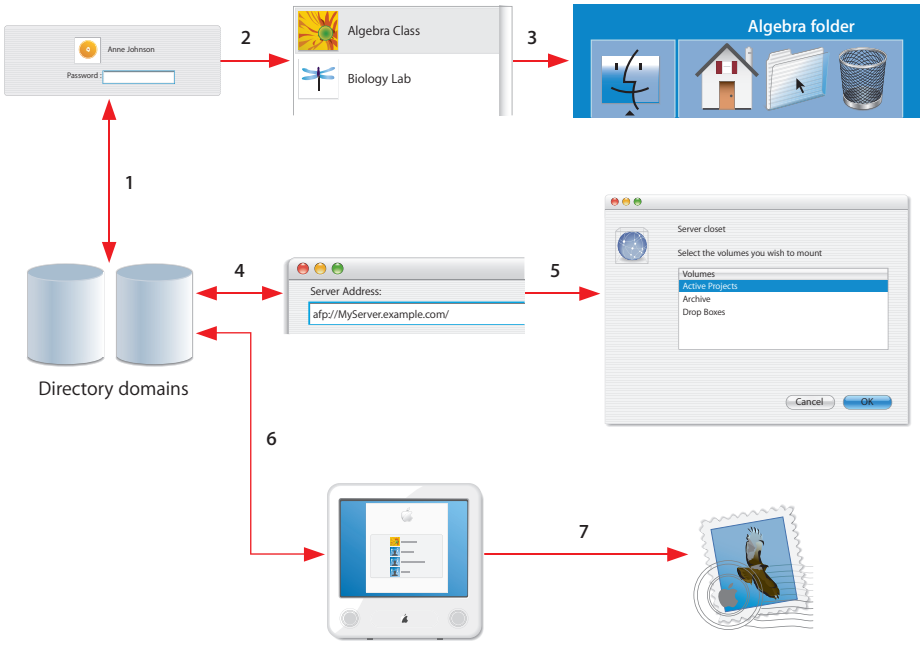
  For example, a K–12 teacher may teach third and fourth grade students in the same classroom. The teacher can create a group for managing the work environment of both classes and nest within it two groups that have settings appropriate for each grade.

- You can use groups to reserve particular computers for use by group members.

  For example, you may want to limit the use of computers in a multimedia lab to only certain students or employees. You'd define a computer list that identifies each computer in the lab. Then you'd restrict access to computers in the computer list to one or more specific groups, such as Marketing or Multimedia.

Groups in Action

Group accounts influence what a user experiences and what a user can do after logging in to or connecting with Mac OS X Server.



1. When a user logs in, Open Directory makes sure the user is defined in a directory domain in the user computer's search path.
2. After login, the preferences associated with the user's workgroup take effect. If the user belongs to more than one workgroup, a list of workgroups appears; choosing one of the workgroups sets up its associated environment.
3. In this example, group preferences have been set up to show the group folder associated with the workgroup in the user's Dock.
4. Group affiliations also control which folders and files a user can access when connecting with a particular server. Open Directory is used to authorize group member access to a particular server.
5. If the user is in the server's search path, a list of share points he or she is authorized to access appears. The list includes share points he or she is authorized to use by being a member of a particular group.
6. You can use computer lists to control which groups can log into a particular computer.

   Just like you can manage preferences for a group, you can also manage preferences for the computer list. One preference is illustrated in the picture above: all users authorized to use the computer are listed in the login window. The user selects a name then enters a password. If Open Directory can authenticate the user, login succeeds.
7. After login, a user can only use services he or she is authorized to use.

   In this example, the user is authorized to use mail service. But you can use Server Admin to deny access to mail, iChat, web, and other services to specific groups or individual users.

Defining Groups

Group accounts, like user accounts and computer lists, can be stored in any Open Directory domain accessible from the Mac OS X computer that needs to access the account. A directory domain can reside on a Mac OS X computer (for example, the LDAP directory of an Open Directory master or a NetInfo domain), or it can reside on a non-Apple server (for example, an LDAP or Active Directory server).

To define a group, you use Workgroup Manager. You can quickly define the group's names, associate a picture with the group for use when workgroups are listed after login, add users or other groups to the group, and set up a group folder.

Using Group Folders

Group folders are for files that group members need to share.

A group folder contains three folders by default: Documents, Library, and Public. The Public folder contains a Drop Box folder. Group folders can be customized, as when you want to use multiple student hand-in (Drop Box) folders or other folders tailored to the needs of the group.

Residing on the server for easy access throughout an organization, a group folder can be shown in the Dock for easy network access anywhere a group member wants to work on group activities.

When you define a group folder, you can designate an owner for the folder. The user who owns the group folder can change group folder attributes in the Finder.

Managing Group Preferences

Managed preferences, defined using Workgroup Manager, allow group members to log into an environment that's appropriate to their needs and consistent from one computer to the next.

For example, a teacher may choose a set of applications and documents that should always be in the Dock for particular classes, or set the system to launch with Simple Finder when a kindergarten student logs in. In a creative environment, Final Cut Pro could always launch when a member of the video editing group logs into any computer. Users' individual and group settings are immediately in effect and they have streamlined access to authorized resources—no matter where they log in.

Group preferences are settings that customize and control a group member's computer experience. Many preferences, such as Dock and Finder preferences, are used to customize the appearance of the desktop. For example, you can set up Dock preferences and Finder preferences so that the work environment of lower-grade students is dramatically simplified. Other preferences are used to manage what a user can access and control. For example, you can set up Media Access preferences to prevent students from burning CDs and DVDs or making changes to a computer's internal disk.

Using Computer Lists

A computer list comprises one or more computers that have the same preference settings and that are available to particular users and groups. Computer lists let you reserve collections of computers for particular groups.

For example, you can use a computer list to reserve high-capacity computers for film students who use Final Cut Pro. You'd assign film students to a group, then set up a computer list for computers you want to reserve for that group's use. A student who isn't a film student (who doesn't belong to the film student group) can't log in to one of those computers.

You create and modify computer lists in Workgroup Manager.

When you set up a computer list, you identify the names and addresses of the computers that will be included in the list. A client computer uses this data to find managed preference information when a user logs in:

- A computer's address must be the "on board," or built-in, Ethernet address, which is unique to each computer. (A computer's Ethernet address is also known as its MAC address.) You can browse for a computer and Workgroup Manager will enter the computer's name and Ethernet address for you.
- You customarily use the computer name specified in a computer's Sharing preferences. If you prefer, you can use a descriptive name that you find more suitable.

Using Groups for Windows Users

You can add Windows users to groups that you create and use the group to manage file access permissions.

A group folder isn't mounted automatically on Windows workstations when group members log in to the Windows domain. If the group folder's share point is shared using SMB/CIFS, a Windows user can go to My Network Places (or Network Neighborhood) and access the contents of the group folder.

For Additional Information

The information you need for defining and managing groups appears in these administration guides:

- The user management guide tells you how to define groups, group folders, and computer lists and how to manage preferences.
- The file services administration guide describes how to set up share points (the access point for group folders and other shared folders) and manage access to them.
- The Windows services administration guide describes how to set up user accounts in a Mac OS X Server directory domain so the server can provide file services, domain login, and home directories to Windows users.

Mail Services

6

Mail services facilitate collaboration among users who use mail applications, also called mail clients.

Mac OS X Server provides standards-based mail services that support Macintosh, Windows, UNIX, and Linux computer users.

How Mail Services Promote Collaboration

Mail services let users send and receive email over a network or across the Internet. They:

- Support standard mail protocols so that users on different kinds of computers can exchange messages and files.

  A standard mail client uses Simple Mail Transfer Protocol (SMTP) to send outgoing email, and Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) to receive incoming email. POP downloads mail messages for storage on user computers. IMAP stores messages on the mail server, so it's useful for people who use more than one computer for email.
- Help eliminate junk mail and viruses.
- Offer security provisions such as user authentication and SSL.
- Let you manage message size, message storage quotas, and other user mail account attributes.
- Support mailing list services. A mailing list is a centralized list of email addresses that users can subscribe to in order to receive announcements and post messages for others in the list. If users have list administration rights, they can also create or maintain lists.

  Mailing lists support communities of users with common interests. Sales people can maintain lists of key customers for sharing with other sales people. Product support and service departments can maintain lists of people interested in information for particular products. Development teams can maintain lists for hosting discussions among team members.

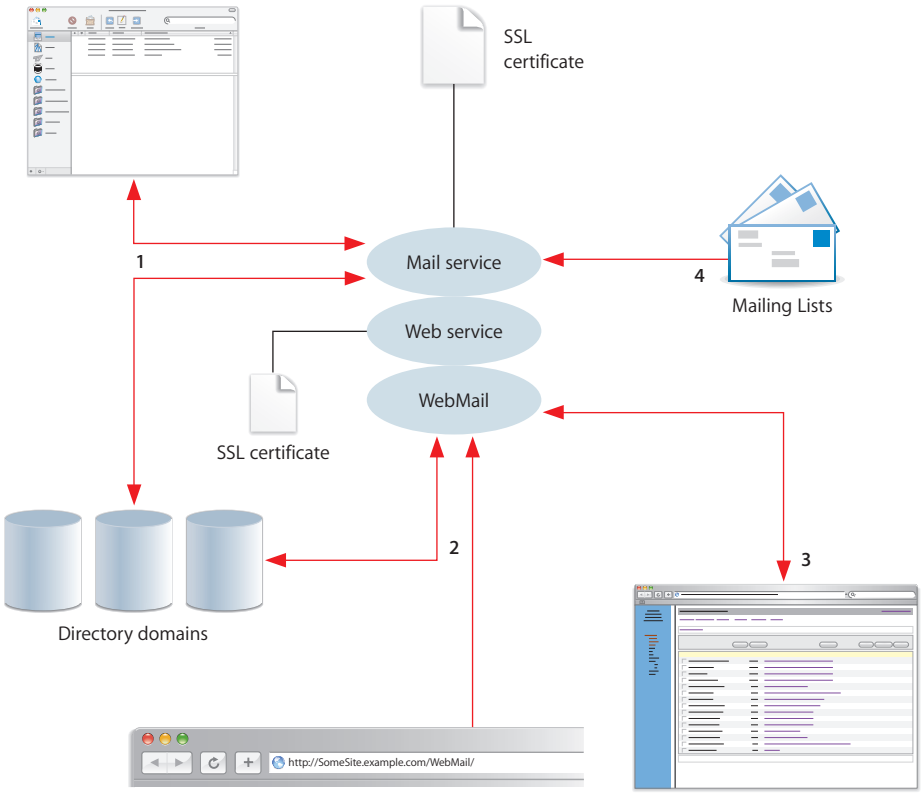
Mail clients can be either email applications that reside on a user's computer or web based, accessible by using a web browser. Mail clients:

- Provide the means by which uses exchange email messages on a one-to-one or one-to-many basis.
- Offer a way to send files by attaching them to messages.
- Expedite following and responding to discussions associated with email threads.
- Support saving and organizing messages for later reference.
- Integrate with address book applications to facilitate saving and finding email addresses.
- Filter junk mail.

Mail Services in Action

Mac OS X Server's mail service uses the high-speed Postfix SMTP mail transfer agent and the scalable Cyrus IMAP and POP services. You can also set up WebMail, a web-based mail service that uses the open-source SquirrelMail project to provide SMTP and IMAP services. The server also provides Mailman for managing mailing lists, including support in Server Admin for creating and maintaining mailing lists.

Both the mail server and WebMail support SSL to safeguard the transport of outgoing and incoming messages. In addition, they both use Open Directory authentication to make sure that mail services are available only for users authorized to use the server. You can also set up mail services so that only particular users and groups are authorized to use them.



1 Each person who uses mail services must have a user account in a directory domain accessible by the server hosting mail service. The short name of the user account is the mail account name; it's used to form the mail address (ShortName@example.com). In addition, each user's account has settings that let you customize how mail service handles mail for the user.

Mail service verifies the identity of users by using Open Directory. A range of authentication options are available, including Kerberos, CRAM-MD5, and APOP.

SSL can be set up for SMTP and for IMAP and POP. With SSL, the server encrypts the data exchanged with mail clients, providing secure, confidential transport of mail messages and attachments.

2 WebMail lets users access their email from any website hosted on the server using SMTP and IMAP. Users open a browser and enter a URL that identifies the site. In the picture above, the URL specifies a site named SomeSite.example.com (http://SomeSite.example.com/WebMail/).

WebMail uses mail service's authentication configuration to validate user identities. If the web site is configured to use SSL, authentication information and messages are encrypted.

3 When a WebMail user enters a valid user name and password, the WebMail window appears. WebMail supports private address books and lets users set up folders for organizing stored messages.

4 Mailing lists can be configured using Server Admin or a web-based interface provided by Mailman. You can configure a list so that users can self-subscribe to it by sending an email to the list (MyMailingList-subscribe@example.com). Or you can configure the list so that only a particular list administrator can designate list subscribers. Mailing list subscribers need not have a mail account on the server or a user account accessible using Open Directory.

Setting Up Mail Service

When you initially set up a server, mail service can be started and configured automatically, but you use Server Admin to fine-tune mail service settings and maintain the mail server:

- If you want users to be able to send and receive mail over the Internet, you should make sure DNS service is set up with the appropriate MX records for your mail service. An ISP can provide this service, or you can set up DNS on your own server.
- Incoming mail service settings influence how mail service handles incoming mail. You choose and enable POP, IMAP, or both, and you select methods for authentication of email clients. You can also set up SSL.
- Outgoing mail service settings primarily focus on configuring SMTP service for sending mail. As for incoming mail, you set up authentication and optionally set up SSL.
- Additional mail service settings let you limit junk mail and viruses, set up mail disk space quota enforcement policies, specify how to handle undeliverable mail, and set up the mail store and database.

Creating Mail Accounts

To make mail service available to users, you configure mail settings in user accounts. For each user, you use Workgroup Manager to:

- Enable mail usage.
- Specify the DNS name or IP address of your mail server.
- Select protocols for retrieving mail (POP, IMAP, or both).
- Set a quota that limits server disk space used for storing the user's mail.
- Configure an alternate mail storage location.

When a user's mail account has been set up, the user configures the email client software to connect to the mail service, providing such information as user name, password, and mail server name or IP address.

Setting Up WebMail

WebMail allows a user to use a web browser, such as Safari, to compose, read, and forward email. Users can also create mail folders for storing messages and manage private address books.

Mac OS X Server's WebMail is provided by a software package called SquirrelMail (www.squirrelmail.org), but requires that mail service (IMAP and SMTP) and web service be set up and running. If web service hosts more than one website, WebMail can provide access to mail service on any or all of the sites. If the site is configured to use SSL, WebMail connections also use it.

WebMail is not enabled by default. To enable WebMail, use Server Admin's web service settings. To configure WebMail, you change SquirrelMail settings.

Using Mailing Lists

Server Admin lets you define mailing lists and manage their memberships. Member privileges you can specify are:

- Subscribe, which lets members subscribe and unsubscribe
- Post, which lets members send messages to the list
- Admin, which lets members modify the list's attributes

List members and administrators can also use Mailman's web-based administration facilities to access other options.

For Additional Information

Several administration guides and websites are related to mail services:

- The mail services administration guide tells you how to set up and manage mail service and mailing lists.
- The web technologies administration guide describes WebMail.
- The network services administration guide tells you how to set up DNS.
- The SquirrelMail website is www.squirrelmail.org.
- The Mailman website is www.list.org.
- The Postfix website is www.postfix.org.
- The Cyrus website is asg.web.cmu.edu/cyrus.

Glossary

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

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.

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

blog See **weblog**.

blogger Someone who publishes information using a weblog.

Blojsom The open-source project on which Weblog service is based.

chatting See **instant messaging**.

computer list A list of computers that have the same preference settings and are available to the same users and groups.

entry A (usually short) article posted on a weblog. Readers can add comments to the entry, but the content associated with the entry can be changed only by the weblog owner. In an LDAP directory, an entry is a collection of attributes (data items) that has a unique distinguished name.

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

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

group folder A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among themselves.

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.

iChat The Mac OS X instant messaging application.

iChat service The Mac OS X Server service that hosts secure chats. iChat service uses Open Directory authentication to verify the identity of chatters and SSL to protect the privacy of users while they chat.

IMAP Internet Message Access Protocol. A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local computer. Mail remains on the server until the user deletes it.

instant messaging Live interactions in which two or more computer users exchange text messages, pictures, audio, or video in real time. Often called chatting because of its spontaneous, conversation-like qualities.

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.

intranet A network of computers operated by and for the benefit of an organization's internal users. Access is commonly restricted to members of the organization. Many times, it refers to a web site for the organization which is accessible only from within the organization. Intranets use the same networking technologies as the Internet (TCP/IP), and sometimes bridge legacy information systems with modern networking technologies.

Jabber/XMPP The open-source protocol used by the jabberd project to provide communication with clients running on a variety of different operating systems. iChat service supports the Jabber/XMPP protocol.

mailing list A mail service used to distribute a single email message to multiple recipients. Mailing list subscribers do not have to be mail users on your mail server. Mailing lists can be administered by someone other than a workgroup or server administrator. Mailing list subscribers can often add or remove themselves from lists.

managed preferences System or application preferences that are under administrative control. Workgroup Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients.

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

nested group A group that is a member of another group. Nested groups enable administrators to manage groups of users at a global level (to influence all members of a group) and at a smaller level (to influence only certain members of a group).

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.

PDA Personal Digital Assistant. A hand-held wireless device that provides personal computing and storage as well as Internet connectivity. PDAs may support date books, address books, email, data messaging, word processing, and other features.

RSS Really Simple Syndication. An XML format that facilitates publicizing, distributing, and gathering web-based content. When webpages publish content using RSS (known as RSS feeds), applications called RSS aggregators can discover that content. Safari has a built-in RSS aggregator that lets you organize and browse RSS feeds, including feeds generated by weblogs hosted using Mac OS X Server's Weblog service.

screen name An instant messaging address. It may include both a user name and a chat server address.

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.

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.

SMTP Simple Mail Transfer Protocol. A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

theme A stylesheet that controls the appearance of weblogs hosted by Weblog service.

trackback An electronic link between two weblog entries. A blogger would use a trackback to respond or refer to another blogger's entry. To create a trackback, a blogger posts an entry on his or her weblog and includes in it a link to the other blogger's entry. When you read the other blogger's entry, you can view the contents of the entry that created the trackback and click a link that takes you to the weblog on which that entry is posted.

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.

weblog A webpage that hosts chronologically ordered entries. It functions as an electronic journal or newsletter. Weblog service lets you create weblogs that are owned by individual users or by all members of a group.

Weblog service The Mac OS X Server service that lets users and groups securely create and use weblogs. Weblog service uses Open Directory authentication to verify the identity of weblog authors and readers. If accessed using a website that's SSL enabled, Weblog service uses SSL encryption to further safeguard access to weblogs.

Windows domain The Windows computers on a network that share a common directory of user, group, and computer accounts for authentication and authorization. An Open Directory master can provide the directory services for a Windows domain.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

Index