# Mac OS X Server

iChat Service Administration
For Version 10.5 Leopard

Apple Inc.
© 2007 Apple Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X Server software might reproduce this publication for the purpose of learning to use such software. No part of this publication might be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid-for support services.

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

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

The Apple logo is a trademark of Apple Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple might constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, ColorSync, Final Cut Pro, Mac, Macintosh, Mac OS, QuickTime, Xgrid, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries. Finder and Safari are trademarks of Apple Inc.

UNIX is a registered trademark of The Open Group.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products.

019-0939/2007-09-01

# Contents

Preface 5 About This Guide
5 What's New in Version 10.5
6 What's in this Guide
6 Using Onscreen Help
7 Advanced Server Administration Guides
8 Viewing PDF Guides on Screen
8 Printing PDF Guides
9 Getting Documentation Updates
9 Getting Additional Information

Chapter 1 11 Understanding iChat Service
11 How iChat Works
12 How iChat Users Are Authenticated
13 Using iChat in Small to Medium Organizations
13 Using iChat in Large Organizations
14 Tools for Managing iChat
14 Server Admin
15 Workgroup Manager
15 Command-Line Tools

Chapter 2 17 Setting Up and Managing iChat Service
17 Understanding iChat Screen Names
17 Adding an Account to iChat
17 Using Other Chat Applications
18 Setup Overview
18 Configuring and Starting Open Directory
19 Opening Firewall Ports for iChat Service
19 Turning iChat Service On
19 Setting up iChat
20 Configuring General Settings
21 Configuring Logging Settings
21 Starting iChat
22 Managing iChat

22 Setting Access Control for iChat
22 Setting SACL Permissions for Users and Groups
23 Setting SACL Permissions for Administrators
23 Using SSL for iChat
24 Locating iChat Configuration Files
25 Viewing iChat Logs
25 Turning Auto-Buddy Support On
25 Stopping iChat

Chapter 3 27 **Setting Up Advanced iChat Service Configurations**
27 Linking Multiple Chat Servers (S2S)
27 Setting Up S2S Communication
28 Securing S2S Connections
28 Using Certificates to Secure S2S Communication
29 Creating an Approved Federation Domain List
30 Integrating with Directory Services
30 Setting the iChat Authentication Method
31 Setting Up iChat on Virtually Hosted Domains

Glossary 33

Index 41

# About This Guide

## This guide provides instructions for setting up, configuring, and administering iChat service on Mac OS X Server.

Instant messaging involves live interactions between computer users exchanging text, pictures, audio, and video. Instant messaging is also known as *chatting,* because of its spontaneous, conversation-like qualities. iChat is the Apple instant messaging service that promotes real-time communication and information-sharing between diverse user groups.

Mac OS X Server version 10.5 includes iChat service administration in its suite of services. iChat service administration is preinstalled on Apple servers.

*iChat Service Administration* provides information about:

- "Setting up iChat", on page 19
- "Managing iChat", on page 22
- "Setting Access Control for iChat", on page 22
- "Linking Multiple Chat Servers (S2S)", on page 27
- "Securing S2S Connections", on page 28
- "Setting Up iChat on Virtually Hosted Domains", on page 31

## What's New in Version 10.5

Mac OS X Server v10.5 offers the following major enhancements to iChat service:

- Server-to-server iChat service
- Server Admin interface upgrades
- Jabber2 process support
- Kerberos support
- Auto-buddy support
- Chat service monitoring and diagnostics support
- Chat server backup and restore
- Client chat transcript archiving

## What's in this Guide

This guide includes the following chapters:

- Chapter 1, "Understanding iChat Service," highlights key concepts and provides basic information about iChat messaging in action, iChat messaging in organizations, and overviews of the iChat service.
- Chapter 2, "Setting Up and Managing iChat Service," describes how to set up your iChat service for the first time and how to manage iChat settings and components.
- Chapter 3, "Setting Up Advanced iChat Service Configurations," provides advanced instructions for setting up iChat service server connections and configurations.

In addition, the Glossary provides brief definitions of terms used in this guide.

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

## Using Onscreen Help

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

**To get help for an advanced configuration of Leopard Server:**

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

The onscreen help contains instructions taken from *Server Administration* and other advanced administration guides described in "Advanced Server Administration Guides," next.

**To see the most recent server help topics:**

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

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

## Advanced Server Administration Guides

*Getting Started* covers installation and setup for standard and workgroup configurations of Mac OS X Server. For advanced configurations, *Server Administration* covers planning, installation, setup, and general server administration. A suite of additional guides, listed below, covers advanced planning, setup, and management of individual services. You can get these guides in PDF format from the Mac OS X Server documentation website:

www.apple.com/server/documentation

| This guide... | tells you how to: |
|---|---|
| *Getting Started* and<br>*Mac OS X Server Worksheet* | Install Mac OS X Server and set it up for the first time. |
| *Command-Line Administration* | Install, set up, and manage Mac OS X Server using UNIX command-line tools and configuration files. |
| *File Services Administration* | Share selected server volumes or folders among server clients using the AFP, NFS, FTP, and SMB protocols. |
| *iCal Service Administration* | Set up and manage iCal shared calendar service. |
| *iChat Service Administration* | Set up and manage iChat instant messaging service. |
| *Mac OS X Security Configuration* | Make Mac OS X computers (clients) more secure, as required by enterprise and government customers. |
| *Mac OS X Server Security Configuration* | Make Mac OS X Server and the computer it's installed on more secure, as required by enterprise and government customers. |
| *Mail Service Administration* | Set up and manage IMAP, POP, and SMTP mail services on the server. |
| *Network Services Administration* | Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, NAT, and RADIUS services on the server. |
| *Open Directory Administration* | Set up and manage directory and authentication services, and configure clients to access directory services. |
| *Podcast Producer Administration* | Set up and manage Podcast Producer service to record, process, and distribute podcasts. |
| *Print Service Administration* | Host shared printers and manage their associated queues and print jobs. |
| *QuickTime Streaming and Broadcasting Administration* | Capture and encode QuickTime content. Set up and manage QuickTime streaming service to deliver media streams live or on demand. |
| *Server Administration* | Perform advanced installation and setup of server software, and manage options that apply to multiple services or to the server as a whole. |
| *System Imaging and Software Update Administration* | Use NetBoot, NetInstall, and Software Update to automate the management of operating system and other software used by client computers. |
| *Upgrading and Migrating* | Use data and service settings from an earlier version of Mac OS X Server or Windows NT. |

| This guide... | tells you how to: |
|---|---|
| *User Management* | Create and manage user accounts, groups, and computers. Set up managed preferences for Mac OS X clients. |
| *Web Technologies Administration* | Set up and manage web technologies, including web, blog, webmail, wiki, MySQL, PHP, Ruby on Rails, and WebDAV. |
| *Xgrid Administration and High Performance Computing* | Set up and manage computational clusters of Xserve systems and Mac computers. |
| *Mac OS X Server Glossary* | Learn about terms used for server and storage products. |

## Viewing PDF Guides on Screen

While reading the PDF version of a guide onscreen:

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

## Printing PDF Guides

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

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

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

## Getting Documentation Updates

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

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

  www.apple.com/server/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/server/macosx)—gateway to extensive product and technology information.
- *Mac OS X Server Support website* (www.apple.com/support/macosxserver)—access to hundreds of articles from Apple's support organization.
- *Apple Training website* (www.apple.com/training)—instructor-led and self-paced courses for honing your server administration skills.
- *Apple Discussions website* (discussions.apple.com)—a way to share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Jabber Software Foundation website* (www.jabber.org)—provides information about the open source project that uses the Jabber/XMPP protocol, a protocol supported by iChat. "Jabber" is a trademarked term given to the XMPP protocol by the Jabber Software Foundation.
- *Jabberd2 Installation and Administration Guide* (http://jabberd.jabberstudio.org/2/docs/)—provides jabberd documentation. Jabberd is the software that Apple uses for implementing the Jabber protocol.

# Understanding iChat Service

# 1

## Mac OS X iChat service provides secure instant messaging for users supported by Mac OS X Server.

iChat is a service that permits users to collaborate by chatting and sharing information using instant messaging and data transfer. This real-time interaction between computer users promotes collaboration without the delay of mail responses and blog postings or the expense of telephone communication or face-to-face meetings.

This collaboration might include:

- Brainstorming solutions, making plans, reporting progress, and exchanging design images
- Exchanging weblinks and files for use as real-time references, or for follow-up viewing
- Generating iChat transcripts when you want a written record of interactions without taking notes
- Conducting weekly staff or project meetings, which can also facilitate collaboration among geographically-dispersed team members
- Using built-in computer microphones for audio chat
- Using video cameras for videoconferencing—a direct, personal, and engaging form of collaboration.

## How iChat Works

iChat provides secure person-to-person instant messaging and chat-room services using standard Extensible Messaging and Presence Protocol (XMPP) which is found in many instant-messaging servers such as Google Talk, Wildfire, and Jabber.

The core of iChat is open source Jabber v2.0, which provides user-presence information (status, icons, and so on) and basic text-message exchange between users or groups (via chat rooms). iChat chat-room features are provided transparently by the Jabber Multi-User (MU) conference module.

Apple uses the jabberd software, which implements the Jabber protocol. *Jabber* is a trademarked term given to this XMPP protocol by the Jabber Software Foundation.

iChat provides peer-file transfer between users that can't establish direct connections to a network because of intervening firewalls that block such connections. In the case of firewalls, iChat acts as a file-transfer proxy, using the Jabber Proxy65 module.

To access messaging and file transfer services, users connect to iChat from various compatible instant messaging (IM) applications. When connected, users can receive information about the status of other subscribed users, exchange messages with users or groups (via chat rooms), or exchange files with users.

Additionally, users can send messages to offline users. These messages are held by iChat and delivered when offline users connect to the server.

iChat also *federates*, or unites with other iChat servers or any XMPP-compliant service (such as Google Talk) using the server-to-server (S2S) capabilities of XMPP. This allows users with accounts on iChat servers to exchange text messages or files with users whose accounts are maintained outside their local network infrastructure, as long as those servers are accessible via the Internet.

To communicate with outside servers, iChat uses a program called S2S, part of the suite of programs that comprise the Jabber v2.0 server, to establish mutual connections with them.

iChat can be configured to require that S2S sessions be encrypted and to block S2S sessions with servers that do not support encryption. For encrypted sessions to be established, both servers must possess public key certificates, either self-signed or issued by a recognized Certificate Authority (CA).

Mac OS X Server includes a preinstalled, default, self-signed certificate, and accepts self-signed certificates from other servers. Depending on the XMPP software vendor at the other end of the S2S connection, a certificate from a trusted authority might need to be installed on the server before S2S sessions can be established.

For more information about increasing server security, see *Mac OS X Server Security Configuration*. Certificate information can also be found in *Server Administration*.

## How iChat Users Are Authenticated

To use iChat on a specific server, users must be defined in directories that the server uses to authenticate users. In addition, iChat uses Secure Socket Layer (SSL) to protect the privacy of users while they chat. The following describes the process of iChat user authentication:

### Step 1: Initiating a chat

To start a chat with another user, you must first know the user's short name and the domain name that iChat is configured to use.

### Step 2: Verifying identity

iChat verifies the identity of users by using Open Directory authentication. Users are authenticated only if they're defined in a directory domain in the server's Open Directory search path.

### Step 3: Authorizing the user

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

### Step 4: Processing URLs

Users can send files and URLs back and forth, making it easy to jointly review information. Because URLs are text, they are passed as normal messages by themselves, or in the body of larger text messages. URLs are unique in that they are recognized and handled differently when displayed in the chat window. Conversely, files are not text and are handled through a different exchange that requires the receiving user to approve the file transfer before it can occur.

### Step 5: Recording a chat

A transcript of chats can be recorded and saved for later use.

## Using iChat in Small to Medium Organizations

For instant messaging in small to medium organizations, you can choose the standard configuration of Mac OS X Server during the installation process. When using a standard configuration, you should use Server Preferences to administer iChat which permits quick and easy configuration.

When using the standard configuration, iChat supports an Auto-buddy feature. The auto-buddy feature automatically adds or deletes users to your iChat buddy list when they are added or deleted in Server Preferences. For more information, see "Turning Auto-Buddy Support On" on page 25.

For more information about setting up iChat in a standard configuration, see *Getting Started*.

## Using iChat in Large Organizations

You can configure and manage iChat service using Server Admin in the advanced configuration of Mac OS X Server v10.5. For more information, see Chapter 2, "Setting Up and Managing iChat Service."

You can also use Server Admin to create customized iChat configurations depending on your organizations requiremenets. For more details, see Chapter 3,"Setting Up Advanced iChat Service Configurations."

This includes setting up a server-to-server federation. When the server-to-server federation is enabled, communication with most other XMPP-compliant chat servers is also established, including the ability to federate with Google Talk. For servers on different networks to communicate, administrators must configure domain name server (DNS), network address translation (NAT), and firewalls, as needed. To use Server Admin for an advanced configuration of iChat, see "Setting Up S2S Communication" on page 27.

Server Admin offers additional options for securing server-to-server communication. This includes using certificates and filtering who has access to iChat service. For more information, see "Securing S2S Connections" on page 28.

## Tools for Managing iChat

Workgroup Manager and Server Admin provide a graphical interface for managing iChat in Mac OS X Server. In addition, you can manage iChat from the command line using Terminal.

These applications are included with Mac OS X Server and can be installed on other computers with Mac OS X v10.5 or later, making those computers administrator computers. For more information about setting up an administrator computer, see the server administration chapter of *Getting Started*.

### Server Admin

Server Admin provides tools to help you set up, manage, and monitor iChat and other services. Use Server Admin to:

- Set up Mac OS X Server as an iChat server. For instructions, see "Setting up iChat" on page 19.
- Manage and monitor iChat service. For instructions, see "Managing iChat" on page 22.

For more information about using Server Admin, see *Server Administration*. This includes information such as:

- Opening and authenticating in Server Admin
- Working with specific servers
- Administering services
- Using SSL for remote server administration
- Customizing the Server Admin environment

Server Admin is installed in the /Applications/Server/ folder.

## Workgroup Manager

Workgroup Manager provides comprehensive management of Mac OS X Server clients and users.

For basic information about using Workgroup Manager, see *User Management*. This includes information such as:

- Opening and authenticating in Workgroup Manager
- Administering accounts
- Customizing the Workgroup Manager environment

Workgroup Manager is installed in the /Applications/Server/ folder.

## Command-Line Tools

Command-line tools are available for administrators who prefer using command-line server administration. For remote server management, submit commands in a secure shell (SSH) session. You can enter commands on Mac OS X servers and computers using the Terminal application, located in the /Applications/Utilities/ folder.

For more information about command-line tools, see *Command-Line Administration*.

# Setting Up and Managing iChat Service

# 2

## This chapter describes how to set up and manage iChat in Mac OS X Server.

This chapter helps you perform the initial iChat service setup and provides information about using, managing, and administering iChat.

## Understanding iChat Screen Names

iChat screen names are Jabber IDs and use the general format *user-short-name@iChat-domain-name* (for example, nancy@ichat.example.com). The *user-short-name* component is the short name of a user defined in the Open Directory search path of the server hosting the iChat service. The *iChat-domain-name* component identifies the server hosting iChat.

To use iChat, you must have a Jabber ID and you must know the Jabber IDs of everyone you want to chat with. Your Jabber ID is created when your user account is created in Open Directory.

## Adding an Account to iChat

When you first run iChat and enter the initial setup information, you can use the iChat > Preferences pane to create your account. For instructions, see iChat help.

After you add your account information you can then add other users to your buddy list. Because buddy lists are saved on the server, they're always available when you start iChat.

## Using Other Chat Applications

You can use other instant messaging applications with iChat as long as the application supports the Jabber protocol. iChat supports instant messaging applications on Windows, Linux, and popular personal digital assistants (PDAs).

## Setup Overview

Here is an overview of the steps for setting up iChat service:

**Step 1:** **Configure and start Open Directory**

iChat uses Open Directory to authenticate users and must be configured before setting up iChat. See "Configuring and Starting Open Directory" on page 18.

**Step 2:** **(Optional) Set up Firewall service**

If you are using a firewall, iChat requires specific ports to be open for iChat features to function. See "Opening Firewall Ports for iChat Service" on page 19.

For more information about Firewall service, see *Network Services Administration*.

**Step 3:** **Turn iChat service on**

Before you configure iChat, turn it on. See "Turning iChat Service On" on page 19.

**Step 4:** **Configure iChat General settings**

Configure the General settings to add host domains, select an SSL certificate, choose your authentication method, and enable XMPP server-to-server federation. See "Configuring General Settings" on page 20.

**Step 5:** **Configure iChat Logging settings**

Use Logging settings to specify where to archive the iChat message logs. See "Configuring Logging Settings" on page 21.

**Step 6:** **Start iChat**

Start iChat on the server using Server Admin. See "Starting iChat" on page 21.

## Configuring and Starting Open Directory

iChat uses Open Directory to authenticate users and service access control lists (SACLs) to verify that users are authorized to use iChat. For more information about configuring Open Directory, see *Open Directory Administration*.

Before you can use iChat:

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

After you log in to iChat, you can chat with any other users who have access to the same iChat server or who are reachable using server-to-server federation, if it is enabled.

For more information about search paths and iChat service authentication, see "Setting Access Control for iChat" on page 22.

## Opening Firewall Ports for iChat Service

iChat requires specific ports to be open on your server. If you have a firewall configured or you are using the Mac OS X Server firewall, you must enable these ports before you can use iChat.

Depending on the iChat functions you require, make sure the following ports are open.

| Ports | Description |
|---|---|
| 16384-16403 | iChat audio/video RTP and RTCP |
| 5060 | iChat Session Initiation Protocol |
| 5190 | iChat Instant Messenger, file transfer |
| 5222 | iChat Server |
| 5223 | iChat Server SSL |
| 5269 | iChat Server server-to-server |
| 5297, 5678 | iChat local UDP |
| 5298 | iChat local |
| 7777 | iChat Server file transfer proxy |

If you run iChat service on a secure network behind a firewall, you don't need to configure firewall settings as long as communication between users is within the network. Firewall settings are required when communicating outside the firewall.

For more information about the Firewall service and settings, see *Network Services Administration*.

## Turning iChat Service On

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

**To turn iChat service on:**

1 Open Server Admin and connect to the server.

2 Click Settings, then click Services.

3 Select the iChat checkbox.

4 Click Save.

### From the Command Line

You can also start iChat service using the `serveradmin` command in Terminal. For more information, see *Command-Line Administration*.

## Setting up iChat

There are two groups of settings on the Settings pane for iChat in Server Admin:

- **General.** Use to set host domains, SSL certificate, authentication method, and XMPP server-to-server federation for iChat.
- **Logging.** Use to configure message log settings for iChat.

The following sections describe how to configure these settings, and a final section tells you how to start iChat when you finish.

## Configuring General Settings

You use the General settings pane in iChat to add host domains, choose an SSL certificate and authentication method, and configure XMPP server-to-server federation settings.

**To configure iChat General settings:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 Click the Add (+) button to add host domains.

The Host Domains list designates the domain names you want iChat to support. Initially, the server host name is shown. You can add or remove other names that resolve to the iChat service IP address such as aliases defined in DNS. When starting iChat you must specify a DNS for the service.

Host domains are used to construct Jabber IDs, which identify iChat users. An example of a Jabber ID is nancy@example1.apple.com.

6 From the SSL Certificate pop-up menu, choose an SSL certificate.

The menu lists all SSL certificates that have been installed on the server.

To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.

For more information about increasing server security, see *Mac OS X Server Security Configuration*. Information about creating and managing server certificates can also be found in *Server Administration*.

7 Choose the method of authentication from the Authentication pop-up menu.

Choose Standard if you want iChat to only accept password authentication.

Choose Kerberos if you want iChat to only accept Kerberos authentication.

Choose Any Method if you want iChat to accept password and Kerberos authentication.

8 To permit iChat to communicate with other XMPP-compliant chat servers, select “Enable XMPP server-to-server federation.”

9 If you are using a certificate with iChat, select "Require secure server-to-server federation."

This option requires an SSL certificate to be installed, which is used to secure the server-to-server federation. For more information, see "Securing S2S Connections" on page 28.

10 To permit unrestricted server-to-server communication, select "Allow federation with all domains."

11 To restrict server-to-server communication to servers that are listed, select "Allow federation with the following domains."

You can add or remove domains using the Add (+) or Delete (–) buttons below the list.

For more information about server-to-server communication, see "Linking Multiple Chat Servers (S2S)" on page 27.

12 Click Save.

## Configuring Logging Settings

Use Server Admin to configure iChat to automatically save chat messages in a location of your choice and to specify when to archive the message log.

**To set up iChat to log chat sessions:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click iChat and then click Settings.

4 Click the Logging button.

5 Select "Automatically save chat messages" to keep a record of user chat messages sent over network.

6 In the Location field, enter a location or click Choose to browse to a folder where you want to save the chat message logs.

7 Select "Archive saved messages every __ day(s)" and enter a number in the field to archive the saved chat message logs on a schedule.

The number is the interval of days between each archive.

Archiving saves disk space by compressing older message logs. The compressed message archives are saved indefinitely until removed by the administrator.

8 Click Save.

## Starting iChat

Use Server Admin to start iChat service. After you start iChat, it restarts when the server restarts.

**To start iChat service:**

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

   The list of services appears.
3. In the expanded Servers list, click iChat.
4. Click Start iChat (below the Servers list).

## Managing iChat

In this section you learn about day-to-day tasks you might perform after you set up iChat on your server. Initial setup information appears in “Setting up iChat” on page 19.

### Setting Access Control for iChat

You can control who can use iChat using Open Directory authentication and iChat service access settings. Keep in mind the following:

- Only a user or group defined in the Open Directory search path can use iChat. You can permit or restrict access to iChat by adding or removing users and groups to an Open Directory search path.

  For more information about Open Directory and how to use Workgroup Manager to add users to the Open Directory, see *Open Directory Administration* and *User Management*.
- SACLs enable you to specify who has access to iChat. This provides you with greater control over who can use the service and the administrators who have access to monitor and manage the service. iChat requires that authenticated users belong to the iChat SACL.

  For information about setting iChat service access for users and groups, see “Setting SACL Permissions for Users and Groups” on page 22.

  For information about setting iChat service access for administrators, see “Setting SACL Permissions for Administrators” on page 23.
- Users created in Workgroup Manager must be added to the iChat SACL (using Server Admin), before they can log into iChat.

### Setting SACL Permissions for Users and Groups

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

**To set user and group SACL permissions for iChat:**

1. Open Server Admin and connect to the server.
2. Click Settings.
3. Click Access.
4. Click Services.

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

   To restrict access to all services, select "For all services."

   To set access permissions for individual services, select "For selected services below" and select the services from the Service list.

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

   To provide unrestricted access, click "Allow all users and groups."

   To restrict access to specific users and groups, select "Allow only users and groups below," click the Add (+) button to open the Users and Groups drawer, and then drag users and groups from the Users and Groups drawer to the list.

7. Click Save.

## Setting SACL Permissions for Administrators

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

**To set administrator SACL permissions for iChat:**

1. Open Server Admin and connect to the server.
2. Click Settings.
3. Click Access.
4. Click Administrators.
5. Select the level of restriction you want for the services:

   To restrict access to all services, select "For all services."

   To set access permissions for individual services, select "For selected services below" and select the services from the Service list.

6. Click the Add (+) button to open the Users and Groups list.
7. Drag users and groups to the list.
8. Set the user's permission:

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

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

9. Click Save.

## Using SSL for iChat

You can maximize the privacy of chats by implementing SSL with iChat. SSL uses a digital certificate to validate the identity of the server and to establish secure, encrypted data exchanges for client-to-server and server-to-server connections.

The digital certificate can be a self-signed certificate or a certificate imported from a certificate authority. For information about defining, obtaining, and installing certificates on your server, see *Server Administration*.

iChat uses SSL to encrypt your chat messages that are sent over the network. However, if your iChat server is logging chat messages, the messages are stored on the server in an unencrypted format. These unencrypted chat messages can be easily viewed by your server administrator. For information about message logging, see "Configuring Logging Settings" on page 21.

**To identify an SSL certificate for use by iChat:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click iChat, then click Settings.

4 From the SSL Certificate pop-up menu, choose the certificate you want iChat to use.

The menu lists all SSL certificates that are installed on the server. To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.

For more information about creating and managing server certificates, see *Server Administration*.

5 Click Save.

## Locating iChat Configuration Files

iChat configuration settings are stored in configuration files that correspond to the main jabberd process and to each of its component processes.

The following is a list of iChat components and their corresponding configuration file location.

| Component | Location |
|---|---|
| jabberd2 (startup script) | /etc/jabberd/jabberd.cfg |
| router (inter-module message routing) | /etc/jabberd/router.xml |
| resolver (domain resolution) | /etc/jabberd/resolver.xml |
| sm (session manager) | /etc/jabberd/sm.xml |
| C2S (client-to-server communications) | /etc/jabberd/c2s.xml |
| S2S (server-to-server communications) | /etc/jabberd/s2s.xml |

These files define settings for the Jabber server and XMPP features supported by Jabber.

## Viewing iChat Logs

You can view iChat logs using Server Admin. iChat logs are located in the following locations:

- The iChat service log is located in /var/log/system.log.
- The iChat file proxy log is located in /private/var/jabberd/log/proxy65.log.
- The iChat multiuser conference log is located in /var/jabberd/log/jcr.log.

**To view iChat logs:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 Click iChat.

4 Click Logs and then choose a log from the View pop-up menu.

## Turning Auto-Buddy Support On

You can configure iChat preferences so that when user accounts are added through Server Preferences, they become buddies. When the users are removed, they are deleted from the buddies list.

Auto-buddy support is only available if the server is installed using the standard configuration. Auto-buddy support is located in Server Preferences.

**To enable Auto-buddy support:**

1 Open the Server Preferences application.

2 Click the iChat button.

3 Select "Automatically make all users buddies."

## Stopping iChat

Use Server Admin to stop iChat.

**To stop iChat:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 In the expanded Servers list, click iChat.

4 Click Stop iChat (below the Servers list).

# Setting Up Advanced iChat Service Configurations

# 3

## This chapter tells you how to customize iChat to create advanced configurations.

iChat provides the following advanced configuration options:

- "Linking Multiple Chat Servers (S2S)" on page 27
- "Securing S2S Connections" on page 28
- "Integrating with Directory Services" on page 30
- "Setting the iChat Authentication Method" on page 30
- "Using Certificates to Secure S2S Communication" on page 28
- "Setting Up iChat on Virtually Hosted Domains" on page 31

## Linking Multiple Chat Servers (S2S)

Use Server Admin to configure an expanded set of options for server-to-server (S2S) communication. For more information, see "Setting Up S2S Communication" on page 27.

Ideally, any server can allow S2S communication, as long as the server is XMPP compliant, accessible to the Internet, and not behind a firewall.

To learn more, see the following topics:

- "Setting Up S2S Communication" on page 27
- "Securing S2S Connections" on page 28

### Setting Up S2S Communication

Use Server Admin to establish S2S communication. When the S2S federation is enabled, communication with most other XMPP-compliant chat servers is enabled, including the ability to federate with Google Talk.

To establish communication between servers on different networks, administrators must configure domain name server (DNS), network address tranlation (NAT), and firewalls, as needed. For more information, see *Network Services Administration*.

Using Server Admin, you can take advantage of additional options for securing S2S communications. These options include filtering domains where servers are matched against a given list.

**To enable or disable S2S communication:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 Select or deselect "Enable XMPP server-to-server federation."

6 Select the "Require secure server-to-server federation" checkbox.

This restricts S2S communication and allow only iChat to connect with servers that support encrypted connections through SSL/TLS. This means that only servers that support TLS are allowed to communicate with your iChat server.

This option requires a Secure Socket Layer (SSL) certificate to be installed, which is used to secure the S2S federation. For more information, see "Securing S2S Connections" on page 28.

7 Set which domains are included in the S2S federation.

Select "Allow federation with all domains" to permit unrestricted S2S communication.

Select "Allow federation with the following domains" to restrict S2S communication to listed servers.

You can add or remove domains using the Add (+) or Delete (–) buttons below the list.

8 Click Save.

## Securing S2S Connections

Using Server Admin, you can take advantage of additional security options for S2S communication. These options include using SSL certificates and filtering domains where servers are matched to those on a given list.

To learn more, see the following topics:

- "Using Certificates to Secure S2S Communication"
- "Creating an Approved Federation Domain List"
- "Integrating with Directory Services"
- "Setting the iChat Authentication Method"

### Using Certificates to Secure S2S Communication

Using Server Admin, you can secure S2S communication with certificates.

By default, iChat selects a port using a preinstalled, self-signed SSL certificate. You can select your own certificate. The selected certificate is used for client-to-server communications on ports 5222 and 5223 and for server-to-server communications.

Jabber provides the following ports:

- 5222 accepts TLS encryption
- 5223 accepts SSL encryption

SSL encrypts your chat message over the network between client-to-server and server-to-server connections. However, if your iChat server is logging chat messages, your messages are stored in a unencrypted format that can be easily viewed by your server administrator. For information about message logging, see "Configuring Logging Settings" on page 21.

**To select a certificate:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 From the SSL Certificate pop-up menu, choose an SSL certificate.

The menu lists all SSL certificates that are installed on the server.

To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.

For more information about creating and managing server certificates, see *Server Administration*.

6 Click Save.

## Creating an Approved Federation Domain List

Server Admin offers the option of configuring an approved list of domains for S2S communication, where only host names and domains that are listed can communicate with your server. This is called a *federation domain list*.

**To create a federation domain list:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 Select "Allow federation with the following domains" to restrict S2S communication to those servers listed.

You can add or remove domains using the Add (+) or Delete (–) buttons below the list.

The entries can be complete host names or domains (this can be a mix of servers and domains).

The server software does the rule-matching to see if these domains can interact. Any domain or host not in the approved list cannot communicate with your iChat server.

6 Click Save.

## Integrating with Directory Services

As with other services, iChat authentication is based on Open Directory or any other Lightweight Directory Access Protocol (LDAP) server bound to the iChat service host.

iChat accesses user accounts through directory services and cannot directly access the LDAP server. You can also bind your server to other LDAP servers, enabling users on the other LDAP servers to authenticate with your iChat server.

For more information, see *Open Directory Administration*.

## Setting the iChat Authentication Method

iChat supports three methods of authentication, with Kerberos authentication being the most secure.

Administrators must use Server Admin to configure an Open Directory master (with Kerberos enabled) to allow Kerberos authentication. Otherwise, the server can be configured to use the Kerberos Domain Controller (KDC) on another host. However, the Kerberos realm hosted by the KDC must match the realm served by the iChat server.

**To select an authentication method:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 Choose the method of authentication from the Authentication pop-up menu.

- Choose Standard if you want iChat to only accept password authentication.
- Choose Kerberos if you want iChat to only accept Kerberos authentication.
- Choose Any Method if you want iChat to accept password and Kerberos authentication.

6 Click Save.

## Setting Up iChat on Virtually Hosted Domains

iChat requires that your host have a host name to be used as the Jabber realm by the iChat server that is resolvable using DNS. This host name is used as the Jabber realm by the iChat server, and clients use this realm to connect to the service.

Clients use a Jabber Identifier (JID) to authenticate and interact with the server. The JID is in the format <user>@<realm> (for example, chatuser@chatserver.example.com). In this example, your iChat service should be configured to host the realm chatserver.example.com.

DNS resolution directs clients to your server when they resolve that host name. To support multiple realms, DNS should be configured appropriately. For more information, see *Network Services Administration*.

**To configure iChat on a virtually hosted domain:**

1 Open Server Admin and connect to the server.

2 Click the triangle to the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 Click Settings, then click General.

5 Change the realms served by iChat by adding a virtual domain to the Host Domains list.

Domains that are added will be supported as Jabber realms.

6 Click Save and restart iChat if necessary.

# Glossary

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

**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's 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.

**Bonjour** A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. Formerly called Rendezvous, this proposed Internet standard protocol is sometimes referred to as ZeroConf or multicast DNS.

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

**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 interacting with the computer (for example, to run programs or modify file system permissions) by entering text commands at a shell prompt. See also **shell**; **shell prompt**.

**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 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 folder with clients on a network.

**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** See **home folder**.

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

**host** Another name for a server.

**host name** A unique name for a computer, historically referred to as the UNIX hostname.

**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.

**Internet** A set of interconnected computer networks communicating through a common protocol (TCP/IP). The Internet 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 data packets and 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. After a user is authenticated, it's possible to access additional services without retyping a password (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.

**Line Printer Remote** See **LPR**.

**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" (For example, bills-computer.local). Although the default name is derived from the computer name, a user can specify this name in the Sharing 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.

**LPR** Line Printer Remote. A standard protocol for printing over TCP/IP.

**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)** 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.

**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 can export shared volumes to computers based on IP address, and also supports single sign-on (SSO) authentication through Kerberos.

**nfsd daemon** An NFS server process that runs continuously behind the scenes and processes NFS protocol and mount protocol requests from clients. nfsd can have multiple threads. The more NFS server threads, the better concurrency.

**Open Directory** The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, Active Directory protocols, or 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 the owner is a member of. 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 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.

**queue** An orderly waiting area where items wait for some type of attention from the system. See also **print queue**.

**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 protocol.

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

**share point** A folder, hard disk (or hard disk partition), or optical disc 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, SMB, NFS (an export), or FTP.

**short name** An abbreviated name for a user. The short name is used by Mac OS X for home folders, 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** Server Message Block. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. SMB services use SMB to provide access to servers, printers, and other network resources.

**TCP** Transmission Control Protocol. A method used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP handles the actual delivery of the data, and TCP keeps track of the 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 on 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 folder 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.

**USB** Universal Serial Bus. A standard for communicating between a computer and external peripherals using an inexpensive direct-connect cable.

**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 to the site while the 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

A
access, service 30
accounts, adding 17
administrator 30
administrator, privileges of 23
administrator computer 14
AFP (Apple Filing Protocol) service
 management of 22
After 17
approved list, domain 29, 30
authentication 12, 30
auto-buddy support 25

B
buddies 17, 25
business size and iChat 13, 14

C
certificates 12, 24, 29
chat service. *See* iChat service 5
collaboration service, iChat as 11
command-line tools 15
configuration
 file implementation 24
 organizational considerations 13, 14

D
digital certificates 24
directory services
 domains 29, 30, 31
 Open Directory 18, 30
documentation 7, 8, 9
domains, directory
 approved list 29, 30
 Open Directory 18, 30
 virtual 31

E
encryption 12, 20, 29
Extensible Messaging and Presence Protocol. *See* XMPP

F
file transfer services 12
firewalls, file transfer through 12

H
help, using 6
host name 29, 31

I
iChat service
 as collaboration service 11
 connections 12, 13, 14
 organizational considerations 13, 14
 overview 5, 11
 planning for 18
 saving messages 21
 starting 19
 tools for 14, 15
instant messaging. *See* iChat service

J
Jabber instant messaging project. *See* iChat service
Jabber Proxy65 module 12

K
Kerberos 30

L
LDAP (Lightweight Directory Access Protocol) service 30
logs 21, 25

N
naming conventions, screen names 17

O
Open Directory 18
Open Directory master 30
open source modules, Jabber 11

P
permissions

administrator  23
ports, encryption  29
privileges, administrator  23
public key certificates. *See* certificates

**R**

realms. *See* Kerberos

**S**

S2S connections  12
SACLs (service access control lists)  22
screen names, iChat  17
Secure Sockets Layer. *See* SSL  17
security
access control  30
approved list  29, 30
authentication  12, 30
firewalls  12
s2s sessions  12
SSL  20, 24, 29
TLS  28
*See also* access; authentication
Server Admin  14, 27
Server Preferences  13
server-to-server connections  27, 28
service access control lists. *See* SACLs
setup procedures. *See* configuration
SSL (Secure Sockets Layer)  20, 24, 29

**T**

TLS (Transport Layer Security) protocol  28

**U**

URLs (Uniform Resource Locators)  13
users, buddy control  17, 25

**V**

virtual domains  31

**X**

Xgrid setup  18
XMPP (Extensible Messaging and Presence Protocol)  12