Apple Confidential Beta Draft

Mac OS X Server
iChat Server Administration

For Version 10.6 Snow Leopard

© 2009 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
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.

019-1416/2009-05-29

Contents

About This Guide

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

You will find information about setting up, managing, and monitoring the iChat server, Apple's instant messaging service that promotes real-time communication and information-sharing between diverse user groups.

What's in This Guide

This guide includes the following sections:

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

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

Using Onscreen Help

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

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

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

- Choose Help > Server Admin Help or Help > Workgroup Manager Help to browse and search the help topics.

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

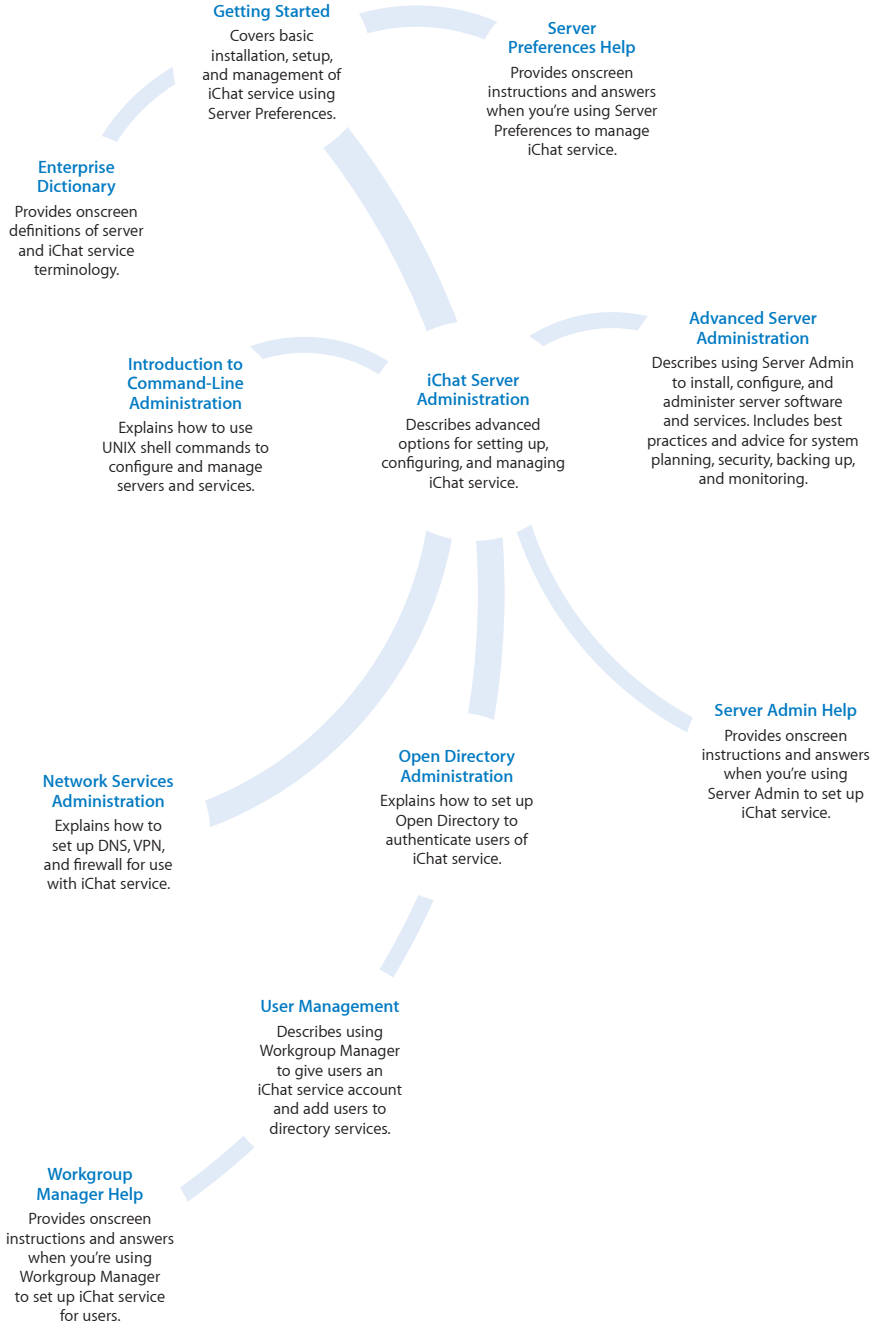
To see the most recent server help topics:

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

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

Documentation Map

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


Getting Started
Covers basic installation, setup, and management of iChat service using Server Preferences.
Server Preferences Help
Provides onscreen instructions and answers when you're using Server Preferences to manage iChat service.
Enterprise Dictionary
Provides onscreen definitions of server and iChat service terminology.
Advanced Server Administration
Describes using Server Admin to install, configure, and administer server software and services. Includes best practices and advice for system planning, security, backing up, and monitoring.
Introduction to Command-Line Administration
Explains how to use UNIX shell commands to configure and manage servers and services.
iChat Server Administration
Describes advanced options for setting up, configuring, and managing iChat service.
Server Admin Help
Provides onscreen instructions and answers when you're using Server Admin to set up iChat service.
Network Services Administration
Explains how to set up DNS, VPN, and firewall for use with iChat service.
Open Directory Administration
Explains how to set up Open Directory to authenticate users of iChat service.
User Management
Describes using Workgroup Manager to give users an iChat service account and add users to directory services.
Workgroup Manager Help
Provides onscreen instructions and answers when you're using Workgroup Manager to set up iChat service for users.

Viewing PDF Guides Onscreen

While reading the PDF version of a guide onscreen:

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

Printing PDF Guides

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

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

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

Getting Documentation Updates

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

- To view new onscreen help topics for a server application, make sure your server or administrator computer is connected to the Internet and click "Latest help topics" or "Staying current" in the main help page for the application.
- To download the latest guides in PDF format, go to the Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.
- An RSS feed listing the latest updates to Mac OS X Server documentation and onscreen help is available. To view the feed, use an RSS reader application such as Safari or Mail and go to:

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

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—get important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx/)—enter the gateway to extensive product and technology information.
- *Mac OS X Server Support website* (www.apple.com/support/macosxserver/)—access hundreds of articles from Apple's support organization.
- *Apple Discussions website* (discussions.apple.com/)—share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com/)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Training and Certification website* (www.apple.com/training/)—hone your server administration skills with instructor-led or self-paced training, and differentiate yourself with certification.
- *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.

Understanding the iChat Service

1

Use this chapter to learn what the iChat service is and how it works.

iChat 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 multiuser (MU) conference module.

Apple uses the jabberd software, which implements the Jabber protocol. *Jabber* is a trademarked term given to XMPP 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 Guide*. Certificate information can also be found in *Advanced 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:

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.

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.

Authorizing the User

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

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.

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 adds or deletes users to your iChat buddy list when they are added or deleted in Server Preferences. For more information, see "Documentation Map" on page 6.

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

Using iChat in Large Organizations

You can configure and manage the iChat server using Server Admin in the advanced configuration of Mac OS X Server v10.6. For more information, see Chapter 2, "Setting Up and Managing the iChat Service."

You can also use Server Admin to create customized iChat configurations depending on your organization requirements. For more details, see Chapter 3, "Setting Up Advanced iChat Server 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 Server-to-Server 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 Server-to-Server 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 v10.6 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 18.
- Manage and monitor the iChat service. For instructions, see "What's in This Guide" on page 5.

For more information about using Server Admin, see *Advanced 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 *Introduction to Command-Line Administration*.

Setting Up and Managing the iChat Service

2

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

This chapter helps you perform the initial iChat server 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 iChat server. The *iChat-domain-name* component identifies the iChat server.

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.

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.

For information, see "Supporting iChat Clients" on page 25.

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:

Configure and start Open Directory

iChat uses Open Directory to authenticate users and must be configured before setting up iChat. See "Printing PDF Guides" on page 8.

(Optional) Set up Firewall Service

If you are using a firewall, iChat requires specific ports to be open for iChat features to function. See "Getting Documentation Updates" on page 8.

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

Turn iChat Service on

Before you configure iChat, turn it on. See "Getting Additional Information" on page 9.

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 iChat General Settings" on page 18.

Configure iChat Logging settings

Use Logging settings to specify where to archive the iChat message logs. See "Configuring Logging Settings" on page 20.

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
1080	SOCKS5 protocol uses this port for file transfers.
5060	iChat Session Initiation Protocol (SIP), required to use audio or video chat.
5190	iChat Instant Messenger. This is the only port required for basic Instant Messenger use.
5222	This port is used for non-TLS or non-SSL connections, as well as SASL and Kerberos (GSSAPI).
5223	This port is for TLS or SSL connections.
5269	This port is used for encrypted TLS or SSL server-to-server connections, as well as nonencrypted connections.
5678	iChat uses this local UDP to determine the user's external IP address.
5297, 5298	Older versions of iChat use this port for BonJour IM. (Mac OS X v10.5 and later use dynamic ports.)
7777	The Jabber Proxy65 module uses this port for iChat Server file transfer proxy.
16402	In Mac OS X 10.5 or later, this port can be used for SIP signaling.
16384–16403	Mac OS X 10.4 and earlier use these ports for audio or video chat. Audio and video packets are sent using RTP and RTCP, and traffic is exchanged in .Mac (MobileMe) to determine the user's external port information.

If you run iChat server 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 the iChat Service On

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

To turn the 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:

- To start the iChat service:

```
$ sudo serveradmin start jabber
```

For information about `serveradmin`, see its man page. For the basics of command-line tool usage, see *Introduction to 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 domain, 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 how to start iChat when you finish.

Configuring iChat 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 at 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 server 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 are 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 *Advanced 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 use 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 Server-to-Server 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.

From the command line:

- To view service settings:

```
$ sudo serveradmin settings jabber
```

The following is an example of the output:

```
jabber:savedChatsArchiveInterval = 7
jabber:enableAutoBuddy = yes
jabber:s2sAllowedDomains = _empty_array
jabber:requireSecureS2S = no
jabber:sslKeyFile = "/etc/certificates/Default.crtkey"
jabber:hosts:_array_index:0 = "pb4server"
jabber:s2sRestrictDomains = no
jabber:eventLogArchiveInterval = 7
jabber:savedChatsLocation = "/var/jabberd/message_archives"
jabber:enableXMPP = yes
jabber:enableSavedChats = no
jabber:welcomeMessage = "Welcome to the iChat Server at pb4server!"
jabber:logLevel = "ALL"
```

- To set service settings:

```
$ sudo serveradmin settings jabber:setting = value
```

Parameter	Description
setting	The name of the setting.
value	The value of the setting.

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

Configuring Logging Settings

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

To start iChat:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 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 perform after you set up iChat on your server. Initial setup information appears in "Setting up iChat" on page 18.

Checking iChat Status

Use Server Admin to check the status of iChat.

To view iChat Status:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 From the expanded Servers list, select iChat.

4 To see information such as whether the service is running, when it started, the servers domain name, and the number of connections, click Overview.

5 To review iChat Service, File Proxy, and Multiuser Conference logs, click Logs.

To choose which log to view, use the View pop-up menu.

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

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 iChat SACL Permissions for Users and Groups" on page 22.

  For information about setting iChat service access for administrators, see "To get the most recent onscreen help for Mac OS X Server:" on page 5.

- Users created in Workgroup Manager must be added to the iChat SACL (using Server Admin), before they can log into iChat.

Setting iChat 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 & Groups window, and then drag users and groups from the Users & Groups window to the list. If you don't see a recently created user, click the Refresh button (below the Servers 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 & Groups window.
7. Drag users and groups to the list from the Users & Groups window.
8. Set the user's permission:
   - To grant administrator access, choose Administer from the Permission pop-up menu next to the user name.
   - To grant monitoring access, choose Monitor from the Permission pop-up menu next to the user name.
9. Click Save.

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 *Advanced Server Administration*.

iChat uses SSL to encrypt 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 20.

To identify an SSL certificate for use by iChat:

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

The list of services appears.

3 Click iChat, then click Settings.

4 Click General.

5 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 *Advanced Server Administration*.

6 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 at 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 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 Groups.

3 From the Groups list, select the group that will use auto-buddy.

4 Click Services.

5 Select the "iChat Auto buddy List" checkbox.

Stopping iChat

Use Server Admin to stop iChat.

To stop iChat:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of services appears.

3 In the expanded Servers list, click iChat.

4 Click Stop iChat (below the Servers list).

5 Click Stop Now.

From the command line:

- To stop iChat service:

```
$ sudo serveradmin stop jabber
```

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

Supporting iChat Clients

This section discusses setting up iChat client settings.

Chatting with Jabber Buddies

If a user has a valid Jabber ID and is registered with a Jabber server, the user can chat with others registered with that Jabber server.

To chat with Jabber buddies:

1. Choose Window > Jabber.
2. To invite a Jabber buddy to chat, double-click his or her buddy picture.

Specifying User Name and Password

iChat lets users communicate using MobileMe, AIM, Google Talk, and Jabber. The steps here explain how to set up an account or get a new one from MobileMe or AIM.

To specify a user's name and password:

1. Choose iChat > Preferences, and then click Accounts.
2. Click the Add (+) button and choose an account type from the Account Type menu.
3. Enter the user name and password:
   - **MobileMe or Mac.com:** Enter the user's full email address (for example, tclark3@me.com or tclark3@mac.com) and password. The password can't be longer than 20 characters.

     To set up a new MobileMe subscription, click "Get an iChat Account."
   - **AIM (AOL Instant Messenger):** Enter the user's AIM screen name (for example, tclark3001) and password.
   - **Jabber:** Enter the user's full Jabber ID (for example, tclark@jabber.org) and password.

     If the Jabber service provider has a specific server name and address or requires a specific port, click the arrow next to Server Options and enter the information.
   - **Google Talk:** Enter the user's Google Talk account name and password.
4. Click Done.

Using a Jabber ID with iChat

If a user has a Jabber account set up, the user can use their Jabber ID with iChat.

To use a Jabber ID with iChat:

1. Choose iChat > Preferences and then click Accounts.
2. Click the Add (+) button.
3. From the Account Type menu, choose Jabber Account.
4. Enter the user's account name and password for their Jabber account and click Done.

Setting Up Advanced iChat Server Configurations

3

Use this chapter to customize iChat to create advanced configurations.

iChat provides the following advanced configuration options:

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 Server-to-Server 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 Server-to-Server 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 translation (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 to a given list.

To enable or disable Server-to-Server communication:

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

   The list of services appears.
3. From the expanded Servers list, select 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 allows 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 Server-to-Server Connections" on page 28.
7. Specify 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 Server-to-Server Connections

Using Server Admin, you can use additional security options to secure server-to-server communications. 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 Server-to-Server Communication" on page 29
- "Creating an Approved Federation Domain List" on page 29
- "Integrating with Directory Services" on page 30
- "Setting the iChat Authentication Method" on page 30

Using Certificates to Secure Server-to-Server Communication

Using Server Admin, you can secure server-to-server 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, which accepts TLS encryption.
- 5223, which 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 an unencrypted format that can be easily viewed by your server administrator. For information about message logging, see "Configure iChat Logging settings" on page 16.

To select a certificate:

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

   The list of services appears.
3. From the expanded Servers list, select 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 *Advanced 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 at 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 server.

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 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: standard, Kerberos, or any.

Kerberos authentication is 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 at 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 uses the format *user@realm* (for example, chatuser@chatserver.example.com). In this example, your iChat server would 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 at 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.

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

Domains that are added supported as Jabber realms.

6 Click Save and restart iChat if necessary.

Index