




# Mac OS X

Security Configuration  
For Version 10.5 Leopard  
Second Edition

 Apple Inc.  
© 2008 Apple Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X software may reproduce this publication for the purpose of learning to use such software. No part of this publication may 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 ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Apple  
1 Infinite Loop  
Cupertino, CA 95014-2084  
408-996-1010  
[www.apple.com](http://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 may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AirPort, AppleScript, AppleShare, AppleTalk, Bonjour, Boot Camp, ColorSync, Exposé, FileVault, FireWire, iCal, iChat, iMac, iSight, iTunes, Keychain, Leopard, Mac, Mac Book, Macintosh, Mac OS, QuickTime, Safari, Xgrid, Xsan, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries.

Apple Remote Desktop, Finder, MacBook Air, QuickTime Broadcaster, Spotlight, and Time Machine are trademarks of Apple Inc.

MobileMe is a service mark of Apple Inc., registered in the U.S. and other countries.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Apple is under license.

Intel, Intel Core, and Xeon are trademarks of Intel Corp. in the U.S. and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

PowerPC™ and the PowerPC logo™ are trademarks of International Business Machines Corporation, used under license therefrom.

UNIX is a registered trademark of The Open Group.

X Window System is a trademark of the Massachusetts Institute of Technology

This product includes software developed by the University of California, Berkeley, FreeBSD, Inc., The NetBSD Foundation, Inc., and their respective contributors.

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.

019-1387/2008-12

# Contents

## Preface

- 11 **About This Guide**
- 11 Target Audience
- 11 What's New in Version 10.5
- 12 What's in This Guide
- 13 Using This Guide
- 13 Using Onscreen Help
- 13 Mac Help
- 14 The Mac OS X Server Administration Guides
- 15 Viewing PDF Guides on Screen
- 15 Printing PDF Guides
- 16 Getting Documentation Updates
- 16 Getting Additional Information
- 17 Acknowledgments

## Chapter 1

- 19 **Introduction to Mac OS X Security Architecture**
- 20 Architectural Overview
- 20 UNIX Infrastructure
- 20 Access Permissions
- 21 Security Framework
- 21 Layered Security Defense
- 22 Credential Management
- 22 Network Security
- 22 Public Key Infrastructure (PKI)
- 23 Authorization Versus Authentication
- 23 Security Features in Mac OS X Leopard
- 23 Mandatory Access Controls
- 24 Sandboxing
- 25 Parental Controls
- 25 Enhanced Protection Against Trojan Applications
- 25 Application-Based Firewall
- 26 Signed Applications
- 26 Smart Card Unlock of FileVault and Encrypted Storage
- 27 Sharing and Collaboration Services

- 27 Enhanced Encrypted Disk Image Cryptography
- 28 Enhanced VPN Compatibility and Integration
- 28 Improved Secure Connectivity

## Chapter 2

- 29 **Installing Mac OS X**
- 29 System Installation Overview
- 29 Disabling the Firmware Password
- 30 Installing from DVD
- 31 Installing from the Network
- 31 Restoring from Preconfigured Disk Images
- 31 Initial System Setup
- 32 Using Setup Assistant
- 32 Creating Initial System Accounts
- 33 Setting Correct Time Settings
- 33 Turn Off Auto-login
- 33 Updating System Software
- 34 Updating from an Internal Software Update Server
- 35 Updating from Internet Software Update Servers
- 36 Updating Manually from Installer Packages
- 37 Verifying the Integrity of Software
- 37 Repairing Disk Permissions
- 38 POSIX Permissions Overview
- 38 ACL Permissions Overview
- 38 Using Disk Utility to Repair Disk Permissions

## Chapter 3

- 41 **Protecting the System Through Hardware**
- 41 Protecting Hardware
- 42 Preventing Wireless Eavesdropping
- 42 Understanding Wireless Security Challenges
- 43 OS Components
- 43 Removing Wi-Fi Support Software
- 44 Removing Bluetooth Support Software
- 45 Removing IR Support Software
- 46 Preventing Unauthorized Recording
- 46 Removing Audio Support Software
- 47 Removing Video Recording Support Software
- 48 Preventing Data Port Access
- 48 Removing USB Support Software
- 49 Removing FireWire Support Software
- 50 System Hardware Modifications
- 50 Authorized AppleCare Certified Technicians

## Chapter 4

- 53 Securing Global System Settings**
- 53 Securing System Startup
- 54 PowerPC-Based Systems
  - 54 Using the Firmware Password Utility
  - 55 Configuring Open Firmware Settings
  - 56 Using Command-Line Tools for Secure Startup
- 56 Intel-Based Macintosh Systems
- 57 Configuring Access Warnings
  - 57 Enabling Access Warnings for the Login Window
  - 58 Understanding the AuthPlugin Architecture
  - 59 Understanding the BannerSample Project
- 59 Enabling Access Warnings for the Command Line

## Chapter 5

- 61 Securing Accounts**
- 61 Types of User Accounts
  - 62 Guidelines for Creating Accounts
  - 62 Defining User IDs
- 63 Securing the Guest Account
- 64 Securing Nonadministrator Accounts
  - 64 Controlling Local Accounts with Parental Controls
  - 66 Securing External Accounts
  - 66 Protecting Data on External Volumes
  - 67 Securing Directory-Based Accounts
- 67 Securing Administrator Accounts
- 68 Securing the System Administrator Account
- 70 Understanding Directory Domains
  - 71 Understanding Network Services, Authentication, and Contacts
  - 72 Configuring LDAPv3 Access
  - 72 Configuring Active Directory Access
- 73 Using Strong Authentication
  - 73 Using Password Assistant to Generate or Analyze Passwords
  - 74 Using Kerberos
  - 75 Using Smart Cards
  - 76 Using Tokens
  - 76 Using Biometrics
- 77 Setting Global Password Policies
- 77 Storing Credentials
  - 78 Using the Default User Keychain
  - 79 Creating Additional Keychains
  - 80 Securing Keychains and Their Items
  - 81 Using Smart Cards as Keychains
  - 82 Using Portable and Network-Based Keychains
- 83 About Certificates

83	Creating a Self-signed Certificate
84	Adding Certificates to a Keychain

## Chapter 6

85	<b>Securing System Preferences</b>
85	System Preferences Overview
87	Securing MobileMe Preferences
89	Securing Accounts Preferences
92	Securing Appearance Preferences
93	Securing Bluetooth Preferences
94	Securing CDs & DVDs Preferences
95	Securing Date & Time Preferences
97	Securing Desktop & Screen Saver Preferences
99	Securing Display Preferences
99	Securing Dock Preferences
100	Securing Energy Saver Preferences
102	Securing Exposé & Spaces Preferences
103	Securing International Preferences
103	Securing Keyboard & Mouse Preferences
105	Securing Network Preferences
106	Securing Parental Controls Preferences
109	Securing Print & Fax Preferences
111	Securing QuickTime Preferences
112	Securing Security Preferences
113	General Security
114	FileVault Security
115	Firewall Security
117	Securing Sharing Preferences
119	Securing Software Update Preferences
120	Securing Sound Preferences
121	Securing Speech Preferences
123	Securing Spotlight Preferences
125	Securing Startup Disk Preferences
126	Securing Time Machine Preferences
128	Securing Universal Access Preferences

## Chapter 7

129	<b>Securing Data and Using Encryption</b>
129	Understanding Permissions
130	Setting POSIX Permissions
130	Viewing POSIX Permissions
131	Interpreting POSIX Permissions
132	Modifying POSIX Permissions
132	Setting File and Folder Flags
132	Viewing Flags

	132	Modifying Flags
	133	Setting ACL Permissions
	133	Modifying ACL Permissions
	134	Changing Global Umask for Stricter Default Permissions
	135	Restricting Setuid Programs
	138	Securing User Home Folders
	139	Encrypting Home Folders
	140	Overview of FileVault
	141	Managing FileVault
	142	Managing the FileVault Master Keychain
	143	Encrypting Portable Files
	143	Creating an Encrypted Disk Image
	144	Creating an Encrypted Disk Image from Existing Data
	145	Creating Encrypted PDFs
	146	Securely Erasing Data
	146	Configuring Finder to Always Securely Erase
	147	Using Disk Utility to Securely Erase a Disk or Partition
	147	Using Command-Line Tools to Securely Erase Files
	148	Using Secure Empty Trash
	148	Using Disk Utility to Securely Erase Free Space
	149	Using Command-Line Tools to Securely Erase Free Space
<b>Chapter 8</b>	151	<b>Securing System Swap and Hibernation Storage</b>
	151	System Swap File Overview
	152	Encrypting System Swap
<b>Chapter 9</b>	153	<b>Avoiding Simultaneous Local Account Access</b>
	153	Fast User Switching
	153	Shared User Accounts
<b>Chapter 10</b>	155	<b>Ensuring Data Integrity with Backups</b>
	155	Understanding the Time Machine Architecture
	155	Deleting Permanently from Time Machine backups
	156	Storing Backups Inside Secure Storage
	156	Restoring Backups from Secure Storage
<b>Chapter 11</b>	157	<b>Information Assurance with Applications</b>
	157	Protecting Data While Using Apple Applications
	157	Mail Security
	158	Enabling Account Security
	159	Remote Content and Hidden Addresses
	160	Disable the Preview Pane for Mail Messages
	160	Signing and Encrypting Mail Messages
	161	Web Browsing Security with Safari

162	Verifying Server Identity
164	Client-Side Authentication
164	Managing Data Communication and Execution
164	Opening Safe Files
165	Nonsecure Forms
165	Syncing Bookmarks
166	AutoFill
167	Controlling Web Content
167	Cookie Storage or Tracking Information
167	Advanced Settings
168	Securing File Downloads
168	Instant Message Security with iChat AV
169	iChat AV Security
169	Enabling Privacy
170	Enabling Encryption Using MobileMe Identity
171	Multimedia Security with iTunes
171	Guest Operating Systems with Boot Camp
172	Protecting Data While Using Apple Services
172	Securing Remote Access Communication
172	VPN Security (L2TP and PPTP)
172	L2TP over IPSec
173	IPSec Configuration
173	Understanding PPTP
174	Network Access Control (802.1x)
174	Securing Internet Communication with Host-Based Firewalls
174	Firewall Protection
175	The Application Firewall
175	Application Firewall Architecture
176	Enabling Advanced Features
176	Firewall Logging
176	Stealth Mode
177	Protection from Unauthorized Applications
178	The IPFW2 Firewall
178	Configuring the IPFW Firewall
178	Understanding IPFW Rulesets
179	Implementing an IPFW Ruleset

## Chapter 12

185	<b>Information Assurance with Services</b>
185	Securing Local Services
185	Securing Bonjour (mDNS)
186	Securing Application Use of Bonjour
186	Address Book
187	iChat AV



187	iPhoto
187	iTunes
187	Securing iDisk Service Access
187	iDisk Service Access
187	Securing Public Folder Access
188	Securing the Back to My Mac (BTMM) Service
188	BTMM Service Architecture
188	Securing BTMM Access
189	Securing Network Sharing Services
189	DVD or CD Sharing
190	DVD or CD Sharing
190	Screen Sharing (VNC)
190	About Screen Sharing
190	Restricting Access to Specific Users
191	File Sharing (AFP, FTP, and SMB)
191	File Sharing
192	Restricting Access to Specific Users
192	Printer Sharing (CUPS)
193	Web Sharing (HTTP)
193	Web Sharing
193	Remote Login (SSH)
194	Restricting Access to Specific Users
194	Enabling an SSH Connection
195	Configuring a Key-Based SSH Connection
198	Preventing Connection to Unauthorized Host Servers
199	Using SSH as a Secure Tunnel
200	Modifying the SSH Configuration File
200	Generating Key Pairs for Key-Based SSH Connections
202	Updating SSH Key Fingerprints
203	Remote Management (ARD)
203	Restricting Access to Specific Users
204	Remote Apple Events (RAE)
204	Restricting Access to Specific Users
205	Xgrid Sharing
205	Restricting Access to Specific Users
206	Internet Sharing
206	Restricting Access to Specific Users
207	Bluetooth Sharing
207	Restricting Access to Specified Users
<b>Chapter 13</b>	<b>209 Advanced Security Management</b>
	209 Managing Authorization Through Rights
	209 Understanding the Policy Database

	209	The Rights Dictionary
	211	The Rules Dictionary
	212	Managing Authorization Rights
	212	Creating an Authorization Right
	212	Modifying an Authorization Right
	213	Example Authorization Restrictions
	213	Example of Authorizing for Screen Saver
	215	Maintaining System Integrity
	215	Validating File Integrity
	216	About File Integrity Checking Tools
	216	Using Digital Signatures to Validate Applications and Processes
	217	Validating Application Bundle Integrity
	217	Validating Running Processes
	217	Activity Analysis Tools
	218	Validating System Logging
	219	Configuring syslogd
	219	Local System Logging
	220	Remote System Logging
	220	Auditing System Activity
	221	Security Auditing
	221	Installing Auditing Tools
	221	Enabling Security Auditing
	222	Analyzing Security Audit Logs
	222	Antivirus Tools
	223	Intrusion Detection Systems
<b>Appendix A</b>	<b>225</b>	<b>Security Checklist</b>
	225	Installation Action Items
	226	Hardware Action Items
	226	Global System Action Items
	227	Account Configuration Action Items
	228	System Preferences Action Items
	229	Encryption (DAR) Action Items
	229	Backup Action Items
	230	Application Action Items
	230	Services Action Items
	230	Advanced Management Action Items
<b>Appendix B</b>	<b>233</b>	<b>Security Scripts</b>
<b>Glossary</b>	<b>243</b>	
<b>Index</b>	<b>255</b>	

# About This Guide

This guide provides an overview of features in Mac OS X that you can use to customize security, known as hardening your computer.

This guide provides instructions and recommendations for securing Mac OS X version 10.5 Leopard or later, and for maintaining a secure computer.

***Important:*** This document is intended for use by security professionals in sensitive environments. Implementing the techniques and setting found in this document will impact system functionality and may not be appropriate for every user or environment.

## Target Audience

This guide is for users of Mac OS X Leopard or later. If you're using this guide, you should be an experienced Mac OS X user, be familiar with the Mac OS X user interface, and have some experience using the Terminal application's command-line interface. You should also be familiar with basic networking concepts.

Some instructions in this guide are complex, and use could cause serious effects on the computer and its security. These instructions should only be used by experienced Mac OS X users, and should be followed by thorough testing.

## What's New in Version 10.5

Mac OS X Leopard offers the following major security enhancements:

- **Better Trojan horse protection.** Mac OS X Leopard marks files that are downloaded to help prevent users from running malicious downloaded applications.
- **Stronger runtime security.** New technologies such as library randomization and sandboxing help prevent attacks that hijack or modify the software on your system.
- **Easier network security.** After you've activated the new Mac OS X Leopard application firewall, it configures itself so you get the benefits of firewall protection without needing to understand the details of network ports and protocols.

- **Improved secure connectivity.** Virtual private network (VPN) support has been enhanced to connect to more of the most popular VPN servers without additional software.
- **Meaningful security alerts.** When users receive security alerts and questions too frequently, they may fall into reflexive mode when the system asks a security-related question, clicking OK without thought. Mac OS X Leopard minimizes the number of security alerts that you see, so when you do see one, it gets your attention.

## What's in This Guide

This guide can assist you in securing a client computer. It does not provide information about securing servers. For help securing computers running Mac OS X version 10.5 Leopard Server or later, see *Mac OS X Server Security Configuration*.

This guide includes the following chapters:

- Chapter 1, "Introduction to Mac OS X Security Architecture," explains the infrastructure of Mac OS X. It also discusses the layers of security in Mac OS X.
- Chapter 2, "Installing Mac OS X," describes how to securely install Mac OS X. The chapter also discusses how to securely install software updates and explains permissions and how to repair them.
- Chapter 3, "Protecting the System Through Hardware," explains how to physically protect your hardware from attacks. This chapter also tells you how to secure settings that affect users of the computer.
- Chapter 4, "Securing Global System Settings," describes how to secure global system settings such as firmware and Mac OS X startup. There is also information on setting up system logs to monitor system activity.
- Chapter 5, "Securing Accounts," describes the types of user accounts and how to securely configure an account. This includes securing the system administrator account, using Open Directory, and using strong authentication.
- Chapter 6, "Securing System Preferences," describes recommended settings to secure Mac OS X system preferences.
- Chapter 7, "Securing Data and Using Encryption," describes how to encrypt data and how to use Secure Erase to verify that old data is completely removed.
- Chapter 8, "Securing System Swap and Hibernation Storage," describes how to secure your system swap and hibernation space of sensitive information.
- Chapter 9, "Avoiding Simultaneous Local Account Access," describes how to further protect fast user switching and local account access to the computer.
- Chapter 10, "Ensuring Data Integrity with Backups," describes the Time Machine architecture and how to securely backup and restore your computer and data.
- Chapter 11, "Information Assurance with Applications," describes how to protect your data while using Apple applications.

- Chapter 12, “Information Assurance with Services,” describes how to secure your computer services.
- Chapter 13, “Advanced Security Management,” describes how to use security audits to validate the integrity of your computer and data.
- Appendix A, “Security Checklist,” provides a checklist that guides you through securing your computer.
- Appendix B, “Security Scripts,” provides a script template for creating a script to secure your computer.

In addition, the Glossary defines terms you’ll encounter as you read 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 This Guide

The following list contains suggestions for using this guide:

- Read the guide in its entirety. Subsequent sections might build on information and recommendations discussed in prior sections.
- The instructions in this guide should always be tested in a nonoperational environment before deployment. This nonoperational environment should simulate, as much as possible, the environment where the computer will be deployed.
- This information is intended for computers running Mac OS X. Before securely configuring a computer, determine what function that particular computer will perform, and apply security configurations where applicable.
- A security checklist is provided in the appendix to track and record the settings you choose for each security task and note what settings you change to secure your computer. This information can be helpful when developing a security standard within your organization.

**Important:** Any deviation from this guide should be evaluated to determine security risks that might be introduced and to take measures to monitor or mitigate those risks.

## Using Onscreen Help

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

## Mac Help

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

On a computer running Mac OS X, you can access onscreen help from the Finder or other applications on the computer. Use the Help menu to open Help Viewer.

## The Mac OS X 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](http://www.apple.com/server/documentation)

This guide...	tells you how to:
<i>Getting Started and Installation &amp; Setup Worksheet</i>	Install Mac OS X Server and set it up for the first time.
<i>Command-Line Administration</i>	Install, set up, and manage Mac OS X Server using UNIX command-line tools and configuration files.
<i>File Services Administration</i>	Share selected server volumes or folders among server clients using the AFP, NFS, FTP, and SMB protocols.
<i>iCal Service Administration</i>	Set up and manage iCal shared calendar service.
<i>iChat Service Administration</i>	Set up and manage iChat instant messaging service.
<i>Mac OS X Security Configuration</i>	Make Mac OS X computers (clients) more secure, as required by enterprise and government customers.
<i>Mac OS X Server Security Configuration</i>	Make Product Name and the computer it's installed on more secure, as required by enterprise and government customers.
<i>Mail Service Administration</i>	Set up and manage IMAP, POP, and SMTP mail services on the server.
<i>Network Services Administration</i>	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, NAT, and RADIUS services on the server.
<i>Open Directory Administration</i>	Set up and manage directory and authentication services, and configure clients to access directory services.
<i>Podcast Producer Administration</i>	Set up and manage Podcast Producer service to record, process, and distribute podcasts.
<i>Print Service Administration</i>	Host shared printers and manage their associated queues and print jobs.
<i>QuickTime Streaming and Broadcasting Administration</i>	Capture and encode QuickTime content. Set up and manage QuickTime streaming service to deliver media streams live or on demand.
<i>Server Administration</i>	Perform advanced installation and setup of server software, and manage options that apply to multiple services or to the server as a whole.

This guide...	tells you how to:
<i>System Imaging and Software Update Administration</i>	Use NetBoot, NetInstall, and Software Update to automate the management of operating system and other software used by client computers.
<i>Upgrading and Migrating</i>	Use data and service settings from an earlier version of Mac OS X Server or Windows NT.
<i>User Management</i>	Create and manage user accounts, groups, and computers. Set up managed preferences for Mac OS X clients.
<i>Web Technologies Administration</i>	Set up and manage web technologies, including web, blog, webmail, wiki, MySQL, PHP, Ruby on Rails, and WebDAV.
<i>Xgrid Administration and High Performance Computing</i>	Set up and manage computational clusters of Xserve systems and Mac computers.
<i>Mac OS X Server Glossary</i>	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 version 10.4 Tiger 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](http://www.apple.com/server/documentation)
- 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:  
[feed://helpox.apple.com/rss/leopard/serverdocupdates.xml](http://helpox.apple.com/rss/leopard/serverdocupdates.xml)

## 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](http://www.apple.com/server/macosx))—gateway to extensive product and technology information.
- *Mac OS X Server Support website* ([www.apple.com/support/macosxserver](http://www.apple.com/support/macosxserver))—access to hundreds of articles from Apple’s support organization.
- *Apple Discussions website* ([discussions.apple.com](http://discussions.apple.com))—a way to share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* ([www.lists.apple.com](http://www.lists.apple.com))—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Customer Training website* ([train.apple.com](http://train.apple.com))—instructor-led and self-paced courses for honing your server administration skills.
- *Apple Certification Programs website* ([train.apple.com/certification/](http://train.apple.com/certification/))—in-depth certification programs designed to create a high level of competency among Macintosh service technicians, help desk personnel, technical coordinators, system administrators, and other professional users.
- *Apple Product Security Mailing Lists website* ([lists.apple.com/mailman/listinfo/security-announce](http://lists.apple.com/mailman/listinfo/security-announce))—mailing lists for communicating by email with other administrators about security notifications and announcements.
- *Open Source website* ([developer.apple.com/opensource/](http://developer.apple.com/opensource/))—access to Darwin open source code, developer information, and FAQs.
- *Apple Product Security website* ([www.apple.com/support/security/](http://www.apple.com/support/security/))—access to security information and resources, including security updates and notifications.



For additional security-specific information, consult these resources:

- *NSA security configuration guides* ([www.nsa.gov/snac/](http://www.nsa.gov/snac/))—The US National Security Agency provides a wealth of information on securely configuring proprietary and open source software.
- *NIST Security Configuration Checklists Repository* ([checklists.nist.gov/repository/category.html](http://checklists.nist.gov/repository/category.html))—This is the US National Institute of Standards and Technology repository for security configuration checklists.
- *DISA Security Technical Implementation Guide* ([www.disa.mil/gs/dsn/policies.html](http://www.disa.mil/gs/dsn/policies.html))—This is the US Defense Information Systems Agency guide for implementing secure government networks. A Department of Defense (DoD) PKI Certificate is required to access this information.
- *CIS Benchmark and Scoring Tool* ([www.cisecurity.org/bench\\_osx.html](http://www.cisecurity.org/bench_osx.html))—The Center for Internet Security benchmark and scoring tool is used to establish CIS benchmarks.

## Acknowledgments

Apple would like to thank the National Security Agency, the National Institute of Standards and Technology, and the Defense Information Systems Agency for their assistance in creating and editing the security configuration guides for Mac OS X Leopard client and server.



Use this chapter to learn about the features in Mac OS X that enhance security on your computer.

Security has never been a more important consideration when selecting a computer platform. Whether you're a home user with a broadband Internet connection, a professional with a mobile computer, or an IT manager with thousands of networked systems, you need to safeguard the confidentiality of information and the integrity of your computers.

With Mac OS X, a security strategy is implemented that is central to the design of the operating system. To enhance security on your computer, Mac OS X provides the following features.

- **Modern security architecture.** Mac OS X includes state-of-the-art, standards-based technologies that enable Apple and third-party developers to build secure software for the Mac. These technologies support all aspects of system, data, and networking security required by today's applications.
- **Secure default settings.** When you take your Mac out of the box, it is securely configured to meet the needs of most common environments, so you don't need to be a security expert to set up your computer. The default settings are designed to make it very difficult for malicious software to infect your computer. You can further configure security on the computer to meet organizational or user requirements.
- **Innovative security applications.** Mac OS X includes features that take the worry out of using a computer. For example, FileVault protects your documents by using strong encryption, an integrated VPN client gives you secure access to networks over the Internet, and a powerful firewall secures your home network.
- **Open source foundation.** Open source methodology makes Mac OS X a robust, secure operating system, because its core components have been subjected to peer review for decades. Problems can be quickly identified and fixed by Apple and the larger open source community.

- **Rapid response.** Because the security of your computer is important, Apple responds rapidly to provide patches and updates. Apple works with worldwide partners, including the Computer Emergency Response Team (CERT), to notify users of potential threats. If vulnerabilities are discovered, the built-in Software Update tool notifies users of security updates, which are available for easy retrieval and installation.

## Architectural Overview

Mac OS X security services are built on two open source standards:

- **Berkeley Software Distribution (BSD).** BSD is a form of UNIX that provides fundamental services, including the Mac OS X file system and file access permissions.
- **Common Data Security Architecture (CDSA).** CDSA provides a wide array of security services, including more specific access permissions, authentication of user identities, encryption, and secure data storage.

## UNIX Infrastructure

The Mac OS X kernel—the heart of the operating system—is built from BSD and Mach.

Among other things, BSD provides basic file system and networking services and implements a user and group identification scheme. BSD enforces access restrictions to files and system resources based on user and group IDs.

Mach provides memory management, thread control, hardware abstraction, and interprocess communication. Mach enforces access by controlling which tasks can send a message to a Mach port. (A Mach port represents a task or some other resource.) BSD security policies and Mach access permissions constitute an essential part of security in Mac OS X, and are both critical to enforcing local security.

## Access Permissions

An important aspect of computer security is the granting or denying of access permissions (sometimes called access rights). A permission is the ability to perform a specific operation, such as gaining access to data or to execute code.

Permissions are granted at the level of folders, subfolders, files, or applications. Permissions are also granted for specific data in files or application functions.

Permissions in Mac OS X are controlled at many levels, from the Mach and BSD components of the kernel through higher levels of the operating system, and—for networked applications—through network protocols.

## Security Framework

The security framework in Mac OS X is an implementation of the CDSA architecture. It contains an expandable set of cryptographic algorithms to perform code signing and encryption operations while maintaining the security of the cryptographic keys. It also contains libraries that allow the interpretation of X.509 certificates.

The CDSA code is used by Mac OS X features such as Keychain and URL Access for protection of login data.

Apple built the foundation of Mac OS X and many of its integrated services with open source software—such as FreeBSD, Apache, and Kerberos, among others—that has been made secure through years of public scrutiny by developers and security experts around the world.

Strong security is a benefit of open source software because anyone can inspect the source code, identify theoretical vulnerabilities, and take steps to strengthen the software.

Apple actively participates with the open source community by routinely releasing updates of Mac OS X that are subject to independent developers' ongoing review—and by incorporating improvements. An open source software development approach provides the transparency necessary to increase Mac OS X security.

## Layered Security Defense

Mac OS X security is built on a layered defense for maximum protection. Security features such as the following provide solutions for securing data at all levels, from the operating system and applications to networks and the Internet.



- Secure worldwide communication—Firewall and mail filtering help prevent malicious software from compromising your computer.

- Secure applications— Encrypted Disk Images and FileVault help prevent intruders from viewing data on your computer.
- Secure network protocols—Secure Sockets Layer (SSL) is a protocol that helps prevent intruders from viewing information exchange across a network, and Kerberos secures the authentication process.
- Security Services—Authentication using keychains, together with POSIX and ACL permissions, helps prevent intruders from using your applications and accessing your files.
- Secure boot and lock down—The Firmware Password Utility helps prevent people who can access your hardware from gaining root-level access permissions to your computer files.

## Credential Management

A keychain is used to store passwords, keys, certificates, and other data placed in the keychain by a user. Due to the sensitive nature of this information, keychains use cryptography to encrypt and decrypt secrets, and they safely store secrets and related data in files.

Mac OS X Keychain services enable you to create keychains and securely store keychain items. After a keychain is created, you can add, delete, and edit keychain items, such as passwords, keys, certificates, and notes for users.

A user can unlock a keychain through authentication (by using a password, digital token, smart card, or biometric reader) and applications can then use that keychain to store and retrieve data, such as passwords.

## Network Security

Secure Transport is used to implement SSL and Transport Layer Security (TLS) protocols. These protocols provide secure communications over a TCP/IP connection such as the Internet by using encryption and certificate exchange.

## Public Key Infrastructure (PKI)

Certificate, key, and trust services include functions to:

- Create, manage, and read certificates
- Add certificates to a keychain
- Create encryption keys
- Manage trust policies

These functions are used when the services call Common Security Service Manager (CSSM) functions. This is transparent to users.

## Authorization Versus Authentication

Authorization is the process by which an entity, such as a user or a computer, obtains the right to perform a restricted operation. Authorization can also refer to the right itself, as in “Anne has the authorization to run that program.” Authorization usually involves authenticating the entity and then determining whether it has the correct permissions.

Authentication is the process by which an entity (such as the user) demonstrates that they are who they say they are. For example, the user, entering a password which only he or she could know, allows the system to authenticate that user. Authentication is normally done as a step in the authorization process. Some applications and operating system components perform their own authentication. Authentication might use authorization services when necessary.

## Security Features in Mac OS X Leopard

Mac OS X Leopard includes the following new security features and technologies to enhance the protection of your computer and your personal information.

- **Enhanced protection against Trojan applications:** Mac OS X Leopard tags and marks downloaded files with first-run warnings to help prevent users from inadvertently running malicious downloaded applications.
- **Runtime protection:** New technologies such as execute disable, library randomization, and sandboxing help prevent attacks that try to hijack or modify the software on your system.
- **Application based firewall:** After you activate the new application firewall, the firewall configures itself to restrict incoming applications for users without requiring the user to write complicated rules.
- **Application signing:** This enables you to verify the integrity and identity of applications on your Mac.

## Mandatory Access Controls

Mac OS X Leopard introduces a new access control mechanism known as mandatory access controls. Although the Mandatory Access Control technology is not visible to users, it is included in Mac OS X Leopard to protect your computer.

Mandatory access controls are policies that cannot be overridden. These policies set security restrictions created by the developer. This approach is different from discretionary access controls that permit users to override security policies according to their preferences.

Mandatory access controls in Mac OS X Leopard aren't visible to users, but they are the underlying technology that helps enable several important new features, including sandboxing, parental controls, managed preferences, and a safety net feature for Time Machine.

Time Machine illustrates the difference between mandatory access controls and the user privilege model—it allows files within Time Machine backups to be deleted only by programs related to Time Machine. From the command line, no user— not even one logged in as root—can delete files in a Time Machine backup.

Time Machine uses this strict policy because it utilizes new file system features in Mac OS X Leopard. The policy prevents corruption in the backup directory by preventing tools from deleting files from backups that may not consider the new file system features.

Mandatory access controls are integrated with the exec system service to prevent the execution of unauthorized applications. This is the basis for application controls in parental controls in Mac OS X Leopard and managed preferences in Mac OS X version 10.5 Leopard Server.

Mandatory access controls enable strong parental controls. In the case of the new sandboxing facility, mandatory access controls restrict access to system resources as determined by a special sandboxing profile that is provided for each sandboxed application. This means that even processes running as root can have extremely limited access to system resources.

## Sandboxing

Sandboxing helps ensure that applications do only what they're intended to do by placing controls on applications that restrict what files they can access, whether the applications can talk to the network, and whether the applications can be used to launch other applications.

In Mac OS X Leopard, many of the system's helper applications that normally communicate with the network—such as mDNSResponder (the software underlying Bonjour) and the Kerberos KDC—are sandboxed to guard them from abuse by attackers trying to access the system.

In addition, other programs that routinely take untrusted input (for instance, arbitrary files or network connections), such as Xgrid and the Quick Look and Spotlight background daemons, are sandboxed.

Sandboxing is based on the system's mandatory access controls mechanism, which is implemented at the kernel level. Sandboxing profiles are developed for each application that runs in a sandbox, describing precisely which resources are accessible to the application.



## Parental Controls

Parental controls provide computer administrators with the tools to enforce a reasonable level of restrictions for users of the computer. Administrator users can use features like Simple Finder to limit the launching of a set of applications or create a white list of web sites that users can visit. This is the kind of simple UI administrators of a public library or computer environment can use to restrict access to applications or sites to keep users from performing malicious activities.

## Enhanced Protection Against Trojan Applications

Applications that download files from the Internet or receive files from external sources (such as mail attachments) can quarantine those files to provide a first line of defense against malicious software such as Trojan horses. When an application receives an unknown file, it adds metadata (quarantine attributes) to the file using new functions found in Launch Services.

Files downloaded using Safari, Mail, and iChat are tagged with metadata indicating that they are downloaded files and referring to the URL, date, and time of the download. This metadata is propagated from archive files that are downloaded (such as ZIP or DMG files) so that any file extracted from an archive is also tagged with the same information. This metadata is used by the download inspector to prevent dangerous file types from being opened unexpectedly.

The first time you try to run an application that has been downloaded, Download Inspector inspects the file, prompts you with a warning asking whether you want to run the application, and displays the information on the date, time, and location of the download.

You can continue to open the application or cancel the attempt, which is appropriate if you don't recognize or trust the application. After an application has been opened, this message does not appear again for that application and the quarantine attributes are lifted.

This new mechanism dramatically reduces the number of warnings related to downloads that you see. Such messages now appear only when you attempt to launch a downloaded application. When you do see a warning, you are given useful information about the source of the download that can help you make an informed decision about whether to proceed.

## Application-Based Firewall

A new application-based firewall makes it easier for nonexperts to get the benefits of firewall protection. The new firewall allows or blocks incoming connections on a per-application basis rather than on a per-port basis.

Users can restrict firewall access to essential network services (such as those needed for DHCP, BOOTP, IPSec VPNs, and Bonjour), or they can allow (or block) access to selected applications on an individual basis. The application firewall uses digital signatures to verify the identity of applications. If you select an unsigned application, Mac OS X Leopard signs that application to uniquely identify it.

For expert users, the IPFW firewall is still available on the system. Because IPFW handles packets at the protocol-layer of the networking stack and the application firewall is an application layer filter, IPFW rules take precedence.

## Signed Applications

By signing applications, your Mac can verify the identity and integrity of an application. Applications shipped with Mac OS X Leopard are signed by Apple. In addition, third-party software developers can sign their software for the Mac. Application signing doesn't provide intrinsic protection, but it integrates with several other features to enhance security.

Features such as parental controls, managed preferences, Keychain, and the firewall use application signing to verify that the applications they are working with are the correct, unmodified versions.

With Keychain, the use of signing dramatically reduces the number of Keychain dialogs presented to users because the system can validate the integrity of an application that uses Keychain. With parental controls and managed preferences, the system uses signatures to verify that an application runs unmodified.

The application firewall uses signatures to identify and verify the integrity of applications that are granted network access. In the case of parental controls and the firewall, unsigned applications are signed by the system on an ad hoc basis to identify them and verify that they remain unmodified.

## Smart Card Unlock of FileVault and Encrypted Storage

Smart cards enable you to carry your digital certificates with you. With Mac OS X, you can use your smart card whenever an authentication dialog is presented.

Mac OS X Leopard has the following four token modules to support this robust, two-factor authentication mechanism and Java Card 2.1 standards:

- Belgium National Identification Card (BEPIC)
- Department of Defense Common Access Card (CAC)
- Japanese government PKI (JPKI)
- U.S. Federal Government Personal Identity Verification, also called FIPS-201(PIV)

Other commercial smart card vendors provide token modules to support integration of their smart card with the Mac OS X Smart Card architecture.

Similar to an ATM card and a PIN code, two-factor authentication relies on something you have and something you know. If your smart card is lost or stolen, it cannot be used unless your PIN is also known.

Mac OS X has additional functionality for smart card use, such as:

- Lock system on smart card removal. You can configure your Mac to lock the system when you remove your smart card.
- Unlock keychain. When you insert a smart card, the keychain can be unlocked and then your stored information and credentials can be used.
- Unlock FileVault. You can use a smart card to unlock your FileVault encrypted home directory. You can enable this function by using a private key on a smart card.

## Sharing and Collaboration Services

In Mac OS X Leopard, you can enable and configure sharing services to allow access only to users that you specify through access control lists (ACLs). You can create user accounts for sharing based on existing user accounts on the system, and for entries in your address book. Sharing services become more secure with ACLs.

## Enhanced Encrypted Disk Image Cryptography

The Disk Utility tool included in Mac OS X enables you to create encrypted disk images—using 128-bit or even stronger 256-bit AES encryption—so you can safely mail valuable documents, files, and folders to friends and colleagues, save the encrypted disk image to CD or DVD, or store it on the local system or a network file server. FileVault also uses this same encrypted disk image technology to protect user folders.

A disk image is a file that appears as a volume on your hard disk. It can be copied, moved, or opened. When the disk image is encrypted, files or folders placed in it are encrypted.

To see the contents of the disk image, including metadata such as file name, date, size, or other properties, a user must enter the password or have a keychain with the correct password.

The file is decrypted in real time, only as the application needs it. For example, if you open a QuickTime movie from an encrypted disk image, Mac OS X decrypts only the portion of the movie currently playing.

## Enhanced VPN Compatibility and Integration

Mac OS X Leopard includes a universal VPN client with support built into the Network preferences pane, so you have everything you need to establish a secure connection. The VPN client supports L2TP over IPSec and PPTP, which make Apple's VPN client compatible with the most popular VPN servers, including those from Microsoft and Cisco.

You can also use digital certificates and one-time password tokens from RSA or CryptoCARD for authentication in conjunction with the VPN client. The one-time password tokens provide a randomly generated passcode number that must be entered with the VPN password—a great option for those who require extremely robust security.

In addition, the L2TP VPN client can be authenticated using credentials from a Kerberos server. In either case, you can save the settings for each VPN server you routinely use as a location, so you can reconnect without needing to reconfigure your system each time.

Apple's L2TP VPN client can connect you to protected networks automatically by using its VPN-on-demand feature. VPN-on-demand can detect when you want to access a network that is protected by a VPN server and can start the connection process for you. This means that your security is increased because VPN connections can be closed when not in use, and you can work more efficiently.

In Mac OS X Leopard, the VPN client includes support for Cisco Group Filtering. It also supports DHCP over PPP to dynamically acquire additional configuration options such as Static Routes and Search Domains.

## Improved Secure Connectivity

VPN support has been enhanced to connect to more of the most popular VPN servers—without additional software.

Use this chapter to install and initialize or update Mac OS X, to repair disk permissions, or to customize your installation to meet your security needs.

Although the default installation of Mac OS X is highly secure, you can customize it for your network security needs. By securely configuring the stages of the installation and understanding Mac OS X permissions, you can harden your computer to match your security policy.

## System Installation Overview

If Mac OS X was already installed on the computer, consider reinstalling it. By reformatting the volume and reinstalling Mac OS X, you avoid vulnerabilities caused by previous installations or settings.

Because some recoverable data might remain on the computer, securely erase the partition you're installing Mac OS X on. For more information, see "Using Disk Utility to Securely Erase a Disk or Partition" on page 147.

If you decide against securely erasing the partition, securely erase free space after installing Mac OS X. For more information, see "Using Disk Utility to Securely Erase Free Space" on page 148.

## Disabling the Firmware Password

Before installing Mac OS X, disable the Extensible Firmware Interface (EFI) password (for Intel-based computers) or the Open Firmware password (for PowerPC-based computers).

If Mac OS X version 10.5 Leopard is already installed, use the Firmware Password Utility to disable the firmware password. For more information, see "Using the Firmware Password Utility" on page 54.

**Note:** If you are using an Intel-based Macintosh computer, you cannot use the following method to disable the EFI password. Use the Firmware Password Utility instead.

**To disable the Open Firmware password:**

- 1 Restart the computer while holding down the Command, Option, O, and F keys.
- 2 When prompted, enter the Open Firmware password.

If you are not prompted to enter a password, the Open Firmware password is disabled.

- 3 Enter the following commands:

```
reset-nvram  
reset-all
```

## Installing from DVD

Before you install Mac OS X, securely erase the partition you want to install Mac OS X on. For more information, see “Using Disk Utility to Securely Erase a Disk or Partition” on page 147.

During installation, install only the packages you plan on using. Removing unused packages frees disk space and reduces the risk of attackers finding vulnerabilities in unused components.

Also, to prevent an attacker from attempting to access your computer during installation, disconnect it from your network.

**To install Mac OS X Leopard from original installation discs:**

**WARNING:** When you install Mac OS X, you erase the contents of the partition you’re installing on. Before continuing, back up the files you want to keep.

- 1 Insert the Mac OS X installation discs in the optical drive.
- 2 Restart the computer while holding down the C key.  
The computer starts up using the disc in the optical drive.
- 3 Proceed through the Installer panes by following the onscreen instructions.
- 4 When the Select a Destination pane appears, select a target disk or volume (partition) and make sure it’s in the expected state.
- 5 Choose a partition to install Mac OS X on, and click Options.
- 6 Select “Erase and Install.”
- 7 In “Format disk as,” choose “Mac OS Extended (Journaled).”  
Mac OS Extended disk formatting provides extended file characteristics that enhance multiplatform interoperability.
- 8 Click OK and then click Continue.

- 9 In the “Install Summary screen,” click Customize and deselect packages you do not plan on using.

Do not select the X11 package unless you use it. The X11 X Window system lets you run X11-based applications in Mac OS X. Although this might be useful, it also makes it harder to maintain a secure configuration. If you use X11, contact your network administrator to securely configure it in your environment.

- 10 Click Install.

## Installing from the Network

There are several ways to deploy images from the network. When choosing a method, make sure you can do it securely. When retrieving the image over a network, make sure the network is isolated and can be trusted. For information about deploying images from a network, see *Server Administration*.

In addition, verify the image to make sure it is correct. For more information about verifying images, see “Verifying the Integrity of Software” on page 37.

## Restoring from Preconfigured Disk Images

One of the most efficient ways to deploy secure computers is to configure a model computer using security settings requested by your organization and then create a disk image to deploy the image on your computers. (For information about how to use Disk Utility to create disk images, see the *System Imaging and Software Update Administration guide*.)

Thoroughly test the settings, making sure the computer meets the standards of your organization, and then create a disk image of the computer. You can then deploy this image to each computer, avoiding the need to manually configure each computer.

You can use NetBoot or Apple Software Restore (ASR) to configure your computer from a network-based disk image:

- With NetBoot, you can install an image directly from the network. For information about how to use NetBoot, see the *System Imaging and Software Update Administration Guide*.
- With ASR, you can install an image deployed by an ASR server, or you can save that image to disk. By saving the image to disk, you can verify its validity before using it. If you’re configuring multiple computers simultaneously, ASR can be much more efficient. For information about how to use ASR, enter `man asr` in a Terminal window.

## Initial System Setup

After installing Mac OS X, the computer restarts and loads Setup Assistant, which you use to initialize your system.

## Using Setup Assistant

Setup Assistant initially configures Mac OS X. You can use Setup Assistant to transfer information from other computers and send registration information to Apple.

Setup Assistant configures the first account on the computer as an administrator account. Administrator accounts should only be used for administration. Users should use standard user accounts for day-to-day computer use.

**Note:** Apple protects information submitted by Setup Assistant, but avoid entering information considered sensitive by your organization.

### To use Setup Assistant without providing confidential information:

- 1 Proceed to the Do You Already Own a Mac screen, select “Do not transfer my information now,” and click Continue.
- 2 Proceed to the Your Internet Connection step and click Different Network Setup.  
If you don’t disable your network connection, an additional step, Enter Your Apple ID, appears. Don’t enter values in the provided fields. The administrator account should only be used for administration, so there’s no need for an Apple ID.
- 3 In Registration Information, press Command-Q and click “Skip to bypass the remaining registration and setup process.”

When you bypass the remaining registration and setup process, you can’t go back to change settings. Before bypassing, you might want to go back through the steps to remove sensitive information.

After you enter information in the Your Internet Connection step, you cannot go back to that step to change your network settings. You can only change network settings after completing installation.

If you enter registration information, an additional step, Register With Apple, appears later in the installation process. Select “Register Later, but don’t register with Apple.”

## Creating Initial System Accounts

After completing the initial steps in Setup Assistant, you’re presented with the Create Your Account step. In this step, you create a system administrator account. Make this account as secure as possible.

**Important:** The system administrator account should be used only when absolutely necessary to perform administrative tasks. Create additional accounts for nonadministrative use. For more information, see “Types of User Accounts” on page 61.

### To set up a secure system administrator account:

- 1 In the Name and Short Name fields, enter names that are not easily guessed.



Avoid names and short names like “administrator” and “admin.” You can use the long or short name when you’re authenticating. The short name is often used by UNIX commands and services.

- 2 In the Password and Verify fields, enter a complex password that is at least 12 characters and composed of mixed-cased characters, numbers, and special characters (such as ! or @).

Mac OS X supports passwords that contain UTF-8 characters or any NUL-terminated byte sequence.

For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.

- 3 In the Password Hint field, do not enter information related to your password.

If a hint is provided, the user is presented with the hint after three failed authentication attempts. Password-related information provided in the field could compromise the integrity of the password. Adding contact information for your organization’s technical support is convenient and doesn’t compromise password integrity.

- 4 Click Continue.

## Setting Correct Time Settings

After creating the system administrator account, you configure the computer’s time settings. You must configure the computer’s time settings correctly because several authentication protocols, such as Kerberos, require valid time settings to work properly. Also, security auditing tools rely on valid time settings.

Mac OS X can set the time by retrieving date and time information from a Network Time Protocol (NTP) server. You should still set valid time settings in case you decide to disable this feature, or in case you don’t have access to a secure internal NTP server.

For more information about using a secure NTP server, see “Securing Date & Time Preferences” on page 95.

## Turn Off Auto-login

Turn off Auto-login to ensure that the system enforces authentication from this point forward during the configuration process.

## Updating System Software

After installing Mac OS X, be sure to install the latest approved security updates. Before connecting your computer to a network to obtain software updates, enable the firewall in Security preferences to allow only essential services.

Mac OS X includes Software Update, an application that downloads and installs software updates from Apple's Software Update server or from an internal software update server.

You can configure Software Update to check for updates automatically. You can also configure Software Update to download, but not install, updates, if you want to install them later.

Before installing updates, check with your organization for their policy on downloading updates. They might prefer that you use an internal software update server, which reduces the amount of external network traffic and lets the organization qualify software updates using organization configurations before updating systems.

**Important:** Security updates published by Apple contain fixes for security issues and are usually released in response to a specific known security problem. Applying these updates is essential.

If Software Update does not install an update that you request, contact your network administrator. Failure to update indicates that the requested update might be a malicious file.

**Important:** If you have not secured and validated settings for network services, do not enable your network connection to install software updates. For information, see Chapter 12, "Information Assurance with Services." Until you securely configure network services settings, you are limited to using the manual method of installing software updates. For more information, see "Updating Manually from Installer Packages" on page 36.

Software updates are obtained and installed in several ways:

- Using Software Update to download and install updates from an internal software update server
- Using Software Update to download and install updates from Internet-based software update servers
- Manually downloading and installing updates as separate software packages

### Updating from an Internal Software Update Server

Your computer can look for software updates on an internal software update server. By using an internal software update server, you reduce the amount of data transferred outside of the network. Your organization can control which updates can be installed on your computer.

If you run Software Update on a wireless network or untrusted network, you might download malicious updates from a rogue software update server. However, Software Update will not install a package that has not been digitally signed by Apple. If Software Update does not install a package, consider the package to be malicious and delete it from `/Library/Updates/`; then download the update again.

You can connect your computer to a network that manages its client computers, which enables the network to require that the computer use a specified software update server. Or, you can modify the `/Library/Preferences/com.apple.SoftwareUpdate.plist` file by entering the following command in a Terminal window to specify your software update server:

#### From the Command Line:

```
# Updating from an Internal Software Update Server
# -----
# Specify the software update server to use.
# Replace swupdate.apple.com with the fully qualified domain name (FQDN)
# or IP address of your software update server.
defaults write com.apple.SoftwareUpdate CatalogURL http://
swupdate.apple.com:8088/index.sucatalog

# Switch your computer back to the default Apple update server.
defaults delete com.apple.SoftwareUpdate CatalogURL
```

## Updating from Internet Software Update Servers

Before connecting to the Internet, make sure your network services are securely configured. For information, see Chapter 12, “Information Assurance with Services.”

If you are a network administrator, instead of using your operational computer to check for and install updates, consider using a test computer to download updates and verify file integrity before installing updates. For more information about verify file integrity, see “Verifying the Integrity of Software” on page 37. You can then transfer the update packages to your operational computer. For instructions on installing the updates, see “Updating Manually from Installer Packages” on page 36.

You can also download software updates for Apple products at [www.apple.com/support/downloads/](http://www.apple.com/support/downloads/).

**Important:** Make sure updates are installed when the computer can be restarted without affecting users accessing the server.

#### To download and install software updates using Software Update:

- 1 Choose Apple () > Software Update.

After Software Update looks for updates to your installed software, it displays a list of updates. To get older versions of updates, go to the software update website at [www.apple.com/support/downloads/](http://www.apple.com/support/downloads/).

- 2 Select the updates you want to install, and choose Update > Install and Keep Package.

When you keep the package, it is stored in the user's Downloads folder (*user\_name/Downloads/*). If you do not want to install updates, click Quit.

- 3 Accept the licensing agreements to start installation.

Some updates might require your computer to restart. If Software Update asks you to restart the computer, do so.

### From the Command Line:

```
# Updating from Internet Software Update Server
# -----
# Download and install software updates.
softwareupdate --download --all --install
```

## Updating Manually from Installer Packages

You can manually download software updates for Apple products from [www.apple.com/support/downloads/](http://www.apple.com/support/downloads/), preferably using a computer designated for downloading and verifying updates. Perform each download separately so file integrity can be verified before installing the updates.

You can review the contents of each security update before installing it. To see the contents of a security update, go to Apple's Security Support Page at [www.apple.com/support/security/](http://www.apple.com/support/security/) and click the Security Updates page link.

### To manually download, verify, and install software updates:

- 1 Go to [www.apple.com/support/downloads/](http://www.apple.com/support/downloads/) and download the software updates on a computer designated for verifying software updates.

**Note:** Updates provided through Software Update might sometimes appear earlier than standalone updates.

- 2 For each update file downloaded, review the SHA-1 digest (also known as a checksum), which should be posted online with the update package.
- 3 Inspect downloaded updates for viruses.
- 4 Verify the integrity of each update.

For more information, see "Verifying the Integrity of Software" on page 37.

- 5 Transfer the update packages from your test computer to your current computer.

The default download location for update packages is */Library/Updates/*. You can transfer update packages to any location on your computer.

6 Double-click the package.

If the package is located in a disk image (dmg) file, double-click the dmg file and then double-click the package.

7 Proceed through the installation steps.

8 If requested, restart the computer.

Install the system update and then install subsequent security updates. Install the updates in order by release date, oldest to newest.

**From the Command Line:**

```
# Updating Manually from Installer Packages
# -----
# Download software updates.
softwareupdate --download --all
# Install software updates.
installer -pkg $Package_Path -target /Volumes/$Target_Volume
```

## Verifying the Integrity of Software

Software images and updates can include an SHA-1 digest, which is also known as a cryptographic checksum. You can use this SHA-1 digest to verify the integrity of the software. Software updates retrieved and installed automatically from Software Update verify the checksum before installation.

**From the Command Line:**

```
# Verifying the Integrity of Software
# -----
# Use the sha1 command to display a file's SHA-1 digest.
# Replace $full_path_filename with the full path filename of the update
# package or image that SHA-1 digest is being checked for.
/usr/bin/openssl sha1 $full_path_filename
```

If provided, the SHA-1 digest for each software update or image should match the digest created for that file. If not, the file was corrupted. Obtain a new copy.

## Repairing Disk Permissions

Before you modify or repair disk permissions, you should understand the file and folder permissions that Mac OS X Server supports. Mac OS X supports the following permissions:

- Portable Operating System Interface (POSIX) permissions—standard for UNIX operating systems.

- Access Control Lists (ACLs) permissions—used by Mac OS X, and compatible with Microsoft Windows Server 2003, Microsoft Windows XP, and Microsoft Windows Vista.

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

## POSIX Permissions Overview

POSIX permissions let you control access to files and folders. Every file or folder has read, write, and execute permissions defined for three categories of users (Owner, Group, and Everyone). You can assign four types of standard POSIX permissions: Read&Write, Read Only, Write Only, None.

For more information, see “Setting POSIX Permissions” on page 130.

## ACL Permissions Overview

An ACL provides an extended set of permissions for a file or folder and enables you to set multiple users and groups as owners.

An ACL is a list of access control entries (ACEs), each specifying the permissions to be granted or denied to a group or user and how these permissions are propagated throughout a folder hierarchy.

In addition, ACLs are compatible with Windows Server 2003, Windows Server 2008, Windows XP, and Windows Vista, giving you added flexibility in a multiplatform environment.

ACLs allow you to be more specific than POSIX when granting permissions. For example, rather than giving a user full write permission, you can restrict the user to the creation of folders but not files.

If a file or folder has no ACEs defined for it, Mac OS X applies standard POSIX permissions. If a file or folder has ACEs defined for it, Mac OS X starts with the first ACE in the ACL and works its way down the list until the requested permission is satisfied or denied.

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

For more information, see “Setting ACL Permissions” on page 133.

## Using Disk Utility to Repair Disk Permissions

Installing software sometimes causes file permissions to become incorrectly set. Incorrect file permissions can create security vulnerabilities. You can use Disk Utility to repair POSIX permissions and minimal ACL permissions.

Most software you install in Mac OS X is installed from package (.pkg) files. Each time something is installed from a package file, a Bill of Materials (.bom) file is created and the installer database is updated. Each Bill of Materials file contains a list of files installed by that package, along with the correct permissions for each file.

When you use Disk Utility to verify or repair disk permissions, it reads the Bill of Materials files from the Mac OS X installation and compares its list to the permissions on each file listed. If the permissions differ, Disk Utility can repair them.

You should repair disk permissions if you experience symptoms that indicate permission-related problems after installing software, software updates, or applications.

**Note:** If you've modified permissions for files in accordance with organizational policies, repairing disk permissions can reset the modified permissions to those stated in the Bill of Materials file. After repairing permissions, reapply the file permission modifications to adhere to your organizational policies.

#### To repair disk permissions:

- 1 Open Disk Utility.
- 2 Select the partition you want to repair.

Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.

- 3 Click Repair Disk Permissions.

If you do not select a partition, this button is disabled.

- 4 Choose Disk Utility > Quit Disk Utility.

#### From the Command Line:

```
# Using Disk Utility to Repair Disk Permissions
# -----
# Repair disk permissions.
diskutil repairPermissions /Volumes/$Target_Boot_Drive
```

**Note:** You can also use the `pkgutil` command to repair specific package permissions. For more information see `pkgutil` man pages.





Use this chapter to secure the system hardware by disabling the Operating System (OS) components and kernel extensions.

After installing and setting up Mac OS X, make sure you protect your system by disabling certain hardware OS components and kernel extensions.

*Important:* This document is intended for use by security professionals in sensitive environments. Implementing the techniques and settings found in this document will impact system functionality and might not be appropriate for every user or environment.

## Protecting Hardware

The first level of security is protection from unwanted physical access. If someone can physically access a computer, it becomes much easier to compromise the computer's security. When someone has physical access to the computer, they can install malicious software or event-tracking and data-capturing services.

Use as many layers of physical protection as possible. Restrict access to rooms that contain computers that store or access sensitive information. Provide room access only to those who must use those computers. If possible, lock the computer in a locked or secure container when it is not in use, and bolt or fasten it to a wall or piece of furniture.

The hard disk is the most critical hardware component in your computer. Take special care to prevent access to the hard disk. If someone removes your hard disk and installs it in another computer, they can bypass safeguards you set up. Lock or secure the computer's internal hardware.

If you can't guarantee the physical security of the hard disk, consider using FileVault for each home folder. FileVault encrypts home folder content and guard against the content from being compromised. For more information, see "Encrypting Home Folders" on page 139.

If you have a portable computer, keep it secure. Lock it up or hide it when it is not in use. When transporting the computer, never leave it in an insecure location. Consider buying a computer bag with a locking mechanism and lock the computer in the bag when you aren't using it.

## Preventing Wireless Eavesdropping

Most network environments have wired and wireless access to the network. Wireless access helps businesses or organizations offer mobility to users throughout their network.

Although wireless technology gives your network more flexibility with your users, it can cause security vulnerabilities you may be unaware of. It is recommended that wherever possible, wireless access be disabled for security reasons. When using a wireless access point, make sure you properly configure the security settings to prevent unauthorized users from attempting to access your network.

Your wireless access point should require encryption of the connection, user authentication (through the use of certificates or smart cards), and time-outs for connections.

By requiring an encrypted wireless connection, you can maintain the integrity and confidentiality of data being transmitted to your wireless access point. The use of certificates or smart cards helps to ensure the users' identity, that your users are who they say they are.

Also, setting a time-out that disconnects wireless user connections lasting longer than 8 to 10 hours prevents your network from being attacked by a computer that is connected through your wireless access point and left unattended.

If you need to use WiFi, see "Network Access Control (802.1x)" on page 174 to leverage 802.1x for securing WiFi traffic.

## Understanding Wireless Security Challenges

Most Mac computers have a built-in wireless network card. Users can configure their computer to be a wireless access point in order to share their Internet connection with other users. However, such a wireless access point isn't usually secure, thereby creating a point of access for an attacker.

Anyone within wireless range can gain access to your network by using an authorized user's insecurely configured wireless LAN. These possible points of access can be very large, depending on the number of users with wireless technology on their computers.

The challenge arises when trying to prevent users from creating access points to your network or trying to identify where the access points are and who is attempting to use them.

Many organizations restrict the use of wireless technology in their network environment. However, most Mac computers have wireless capability built in, and simply turning it off may not meet your organization's wireless technology restrictions. You might need to remove components from Mac OS X to disable them from being turned on in System Preferences.

## OS Components

Special hardware, such as wireless networking cards and audio/video components, need driver software that runs at the kernel level. This driver software is implemented as kernel extensions (“kexts”) in Mac OS X, also known as OS components. These kernel extensions can be removed from Mac OS X to prevent the use of a piece of hardware.

Disabling or removing OS components or kernel extensions will alter the behavior or performance of the system.

**Important:** Mac OS X sometimes has updates to specific OS components. When your computer installs these updates the component is overwritten or reinstalled if it was previously removed. This then reenables the hardware you wanted disabled. When you install updates make sure that the installation does not reenables an OS component you wanted disabled.

## Removing Wi-Fi Support Software

Use the following instructions for removing Airport support. This task requires you to have administrator privileges.

You can also have an Apple Authorized Technician remove Airport hardware from your Apple computer.

**Important:** Repeat these instructions every time a system update is installed.

**To remove kernel extensions for AirPort hardware:**

- 1 Open the /System/Library/Extensions folder.
- 2 Drag the following files to the Trash:
  - AppleAirPort.kext
  - AppleAirPort2.kext
  - AppleAirPortFW.kext
- 3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the `/System/Library/Extensions` folder. When the folder has a new modified date, the Extension cache files (located in `/System/Library/`) are deleted and rebuilt automatically by Mac OS X.

- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

#### From the Command Line:

```
# -----  
# Protecting System Through Hardware  
# -----  
# Removing Wi-Fi Support Software  
# -----  
# Remove AppleAirport kernel extensions.  
srn -rf /System/Library/Extensions/AppleAirport.kext  
srn -rf /System/Library/Extensions/AppleAirport2.kext  
srn -rf /System/Library/Extensions/AppleAirportFW.kext  
# Remove Extensions cache files.  
touch /System/Library/Extensions
```

### Removing Bluetooth Support Software

Use the following instructions to remove Bluetooth support for peripherals such as keyboards, mice, or phones. This task requires you to have administrator privileges.

You can also have an Apple Authorized Technician remove the built-in Bluetooth hardware from your Apple computer.

**Important:** Repeat these instructions every time a system update is installed.

#### To remove kernel extensions for Bluetooth hardware:

- 1 Open the `/System/Library/Extensions` folder.
- 2 Drag the following files to the Trash:

`IOBluetoothFamily.kext`

`IOBluetoothHIDDriver.kext`

- 3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the `/System/Library/Extensions` folder. When the folder has a new modified date, the Extension cache files (located in `/System/Library/`) are deleted and rebuilt by Mac OS X.

- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

## From the Command Line:

```
# Removing BlueTooth Support Software
# -----
# Remove Bluetooth kernel extensions.
srm -rf /System/Library/Extensions/IOBluetoothFamily.kext
srm -rf /System/Library/Extensions/IOBluetoothHIDDriver.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## Removing IR Support Software

Use the following instructions to remove IR hardware support. This task requires you to have administrator privileges.

You can also have an Apple Authorized Technician remove IR hardware from your Apple computer.

**Important:** Repeat these instructions every time a system update is installed.

### To remove kernel extensions for IR hardware support:

- 1 Open the /System/Library/Extensions folder.

- 2 Drag the following file to the Trash:

AppleIRController.kext

- 3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library) are deleted and rebuilt automatically by Mac OS X.

- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

## From the Command Line:

```
# Removing IR Support Software
# -----
# Remove IR kernel extensions.
srm -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## Preventing Unauthorized Recording

Your computer might be in an environment where recording devices such as cameras or microphones are not permitted. You can protect your organization's privacy by disabling these devices. This task requires you to have administrator privileges.

**Note:** Some organizations insert a dummy plug into the audio input and output ports to ensure that audio hardware is disabled.

## Removing Audio Support Software

Use the following instructions to remove support for the microphone and audio subsystem. This may disable audio playback.

You can also have an Apple Authorized Technician remove the built-in microphone hardware from your Apple computer.

**Important:** Repeat these instructions every time a system update is installed.

**To remove kernel extensions for audio hardware:**

- 1 Open the /System/Library/Extensions folder.
- 2 To remove support for audio components such as the microphone, drag the following files to the Trash:  
AppleOnboardAudio.kext  
AppleUSBAudio.kext  
AudioDeviceTreeUpdater.kext  
IOAudioFamily.kext  
VirtualAudioDriver.kext
- 3 Open Terminal and enter the following command:  

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Mac OS X.
- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

## From the Command Line:

```
# Securing Audio Support Software
# -----
# Remove Audio Recording kernel extensions.
srms -rf /System/Library/Extensions/AppleOnboardAudio.kext
srms -rf /System/Library/Extensions/AppleUSBAudio.kext
srms -rf /System/Library/Extensions/AppleDeviceTreeUpdater.kext
srms -rf /System/Library/Extensions/IOAudioFamily.kext
srms -rf /System/Library/Extensions/VirtualAudioDriver.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## Removing Video Recording Support Software

Use the following instructions to remove support for an external or built-in iSight camera.

**Note:** The support for external iSight cameras should be removed on all machines. Removing only support for internal iSight cameras would still leave support for external cameras available.

You can also have an Apple Authorized Technician remove the built-in video camera hardware from your Apple computer.

**Important:** Repeat these instructions every time a system update is installed.

### To remove kernel extensions for video hardware:

- 1 Open the /System/Library/Extensions folder.
- 2 To remove support for the external iSight camera, drag the following file to the Trash:  
Apple\_iSight.kext
- 3 To remove support for the built-in iSight camera, control click the IOUSBFamily.kext and select Show Package Contents.
- 4 Open the /Contents/PlugIns/ folder.
- 5 Drag the following file to the Trash:  
AppleUSBVideoSupport.kext
- 6 Open Terminal and enter the following command:  

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Mac OS X.
- 7 Choose Finder > Secure Empty Trash to delete the file.
- 8 Restart the system.

## From the Command Line:

```
# Securing Video Recording Support Software
# -----
# Remove Video Recording kernel extensions.
# Remove external iSight camera.
rm -rf /System/Library/Extensions/Apple_iSight.kext
# Remove internal iSight camera.
rm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/\
    AppleUSBVideoSupport.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## Preventing Data Port Access

Computer data ports can be easily compromised if your machine is left alone for a long period of time or is stolen. To prevent your machine from being compromised, keep it in a locked environment or hidden when you are not using it.

You can protect your system by preventing an unauthorized user from using your data ports. This prevents users from booting to a different volume using a USB Flash drive, USB, or FireWire external hard drive. This task requires you to have administrator privileges.

Also by setting a firmware password using the Firmware Password Utility, you can prevent a physical Direct Memory Access (DMA) attack over Firewire. When the firmware password is set, any external device is denied direct access to computer memory content. For more information about the Firmware Password Utility, see “Using the Firmware Password Utility” on page 54.

## Removing USB Support Software

Use the following instructions to remove USB mass storage device input/output support such as USB Flash drives and external USB hard drives.

The removal of this kernel extension only affects USB mass storage devices. It does not affect other USB devices such as a USB printer, mouse, or keyboard. This task requires you to have administrator privileges.

**Important:** Repeat these instructions every time a system update is installed.

**To remove kernel extensions for specific hardware:**

- 1 Open the /System/Library/Extensions folder.
- 2 To remove support for USB mass storage devices, drag the following file to the Trash:  
IOUSBMassStorageClass.kext



- 3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the `/System/Library/Extensions` folder. When the folder has a new modified date, the Extension cache files (located in `/System/Library/`) are deleted and rebuilt by Mac OS X.

- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

#### From the Command Line:

```
# Securing USB Support Software
# -----
# Remove USB kernel extensions.
rm -rf /System/Library/Extensions/IOUSBMassStorageClass.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## Removing FireWire Support Software

Use the following instructions to remove Firewire input/output support such as external Firewire hard disks. This task requires you to have administrator privileges.

**Important:** Repeat these instructions every time a system update is installed.

#### To remove kernel extensions for specific hardware:

- 1 Open the `/System/Library/Extensions` folder.
- 2 To remove support for FireWire mass storage devices, drag the following file to the Trash:

`IOFireWireSerialBusProtocolTransport.kext`

- 3 Open Terminal and enter the following command:

```
$ sudo touch /System/Library/Extensions
```

The `touch` command changes the modified date of the `/System/Library/Extensions` folder. When the folder has a new modified date, the Extension cache files (located in `/System/Library/`) are deleted and rebuilt by Mac OS X.

- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

## From the Command Line:

```
# Securing FireWire Support Software
# -----
# Remove FireWire kernel extensions.
srm -rf /System/Library/Extensions/\
    IOFireWireSerialBusProtocolTransport.kext
# Remove Extensions cache files.
touch /System/Library/Extensions
```

## System Hardware Modifications

Removing kernel extensions does not permanently disable components. You need administrative access to restore and reload them.

Although disabling hardware in this manner is not as secure as physically disabling hardware, it is more secure than disabling hardware through System Preferences. This method of disabling hardware components might not be sufficient to meet an organization's security policy. Consult your organization's operational policy to determine if this method is adequate.

### Authorized AppleCare Certified Technicians

If your environment does not permit the use of the following hardware components, you must physically disable them:

- Airport
- Bluetooth
- Microphone
- Camera
- IR Port

**Important:** Attempting to remove components without the use of an Apple Certified technician will void your warranty.

Only an Apple Certified technician can physically disable these components without voiding the warranty on your computer. A limited number of Apple Certified technicians can remove preapproved components.

After an Apple Certified technician removes the component the technician logs a special note with Apple Care, indicating that the computer has had a component properly removed. Most components removed by Apple technicians can be reinstalled, if needed.

To locate a Certified Apple technician go to: [www.apple.com/buy](http://www.apple.com/buy).

Also, see your local Apple representative for more information.

**Note:** If you are in a government organization and need a letter of volatility for Apple products, send your request to [AppleFederal@apple.com](mailto:AppleFederal@apple.com).



Use this chapter to learn how to secure global system settings, secure firmware and Mac OS X startup, and to use access warnings.

After installing and setting up Mac OS X, make sure you protect your hardware and secure global system settings.

## Securing System Startup

When a computer starts up, it first starts Extensible Firmware Interface (EFI) or Open Firmware. EFI is the software link between the motherboard hardware and the software operating system. Open Firmware is similar to EFI, but it runs on PowerPC-based Macintosh computers. EFI and Open Firmware determine which partition or disk to load Mac OS X from. They also determine whether the user can enter single-user mode.

Single-user mode logs in the user as root. This is dangerous because root user access is the most powerful level of access, and actions performed as root are anonymous.

If you create an Open Firmware or EFI password, you prevent users from accessing single-user mode. The password also stops users from loading unapproved partitions or disks and from enabling target disk mode at startup.

After creating an Open Firmware or EFI password, you must enter this password when you start the computer from an alternate disk (for situations such as hard disk failure or file system repair).

To secure startup, perform one of the following tasks:

- Use the Firmware Password Utility to set the Open Firmware password.
- Set the Open Firmware password within Open Firmware.
- Verify and set the security mode from the command line.

**WARNING:** EFI and Open Firmware settings are critical. Take great care when modifying these settings and when creating a secure Firmware password.

An Open Firmware password provides some protection, but it can be reset if a user has physical access to the machine and changes the physical memory configuration of the machine.

Open Firmware password protection can be bypassed if the user changes the physical memory configuration of the machine and then resets the PRAM three times (by holding down Command, Option, P, and R keys during system startup).

For more information about Open Firmware password protection, see:

- AppleCare Knowledge Base article #106482, “Setting up Open Firmware Password protection in Mac OS X 10.1 or later” ([www.apple.com/support/](http://www.apple.com/support/))
- AppleCare Knowledge Base article #107666, “Open Firmware: Password Not Recognized when it Contains the Letter ‘U’” ([www.apple.com/support/](http://www.apple.com/support/))

## PowerPC-Based Systems

PowerPC-based computers use Open Firmware to control hardware. This is similar to the BIOS on an x86 PC. Open Firmware is the hardware base layer for Mac OS X and is a possible point of intrusion. By protecting it from unauthorized access, you can prevent attackers from gaining access to your computer.

### Using the Firmware Password Utility

The Mac OS X installation disc includes the Firmware Password Utility, which you can use to enable an Open Firmware or EFI password.

#### To use the Firmware Password Utility:

- 1 Log in with an administrator account and open the Firmware Password Utility (located on the Mac OS X installation disc in /Applications/Utilities/).
- 2 Click Change.
- 3 Select “Require password to change Open Firmware settings.”

To disable the Open Firmware or EFI password, deselect “Require password to change Open Firmware settings.” You won’t need to enter a password and verify it. Disabling the Open Firmware password is only recommended for installing Mac OS X.

- 4 In the Password and Verify fields, enter a new Open Firmware or EFI password, and click OK.

This password can be up to eight characters.

Do not use the capital letter “U” in an Open Firmware password. If you do, your password will not be recognized during the startup process.

- 5 Close the Firmware Password Utility.

You can test your settings by attempting to start up in single-user mode. Restart the computer while holding down the Command and S keys. If the login window loads, changes made by the Firmware Password Utility were completed successfully.

## Configuring Open Firmware Settings

You can securely configure Open Firmware settings by setting a firmware password.

These instructions only apply to PowerPC-based Macintosh computers. If you are using an Intel-based Macintosh computer, use the Firmware Password Utility instead.

**WARNING:** Modifying critical system files can cause unexpected issues. Your modified files can also be overwritten during software updates. Make these modifications on a test computer first, and thoroughly test your changes every time you change your system configuration.

### To configure Open Firmware settings in Open Firmware:

- 1 Restart the computer while holding down the Command, Option, O, and F keys.

This loads Open Firmware.

- 2 At the following prompt, change the password:

```
> password
```

- 3 Enter a new password and verify it when prompted.

This password can be up to eight characters.

Do not use the capital letter “U” in an Open Firmware password.

- 4 Enable command mode:

```
> setenv security-mode command
```

In command mode the computer starts up from the partition selected in the Startup Disk pane of System Preferences.

You can also enable full mode. Full mode is more restrictive than command mode. After enabling full mode, Open Firmware commands require you to enter your Open Firmware password. This includes the `boot` command, so Mac OS X will not start up unless you enter `boot` and authenticate with the Open Firmware password.

To enable full mode, enter:

```
> setenv security-mode full
```

- 5 Restart the computer and enable Open Firmware settings with the following command:

```
> reset-all
```

The login window should appear after restarting.

To test your settings, attempt to start up in single-user mode. Restart the computer while holding down the Command and S keys. If the login window appears, your Open Firmware settings are set correctly.

## Using Command-Line Tools for Secure Startup

You can also configure Open Firmware or EFI from the command line by using the `nvrnm` tool. However, only the `security-mode` environment variable can be securely set.

You can set the security mode to one of the following values:

- **None:** This is the default value of `security-mode` and provides no security to your computer's Open Firmware.
- **Command:** This value requires a password if changes are made to Open Firmware or a user attempts to start up from an alternate volume or device.
- **Full:** This value requires a password to start up or restart your computer. It also requires a password to make changes to Open Firmware.

For example, to set the `security-mode` to `full` you would use the following command:

```
$ sudo nvram setsecurity-mode=Full
```

Do not set the `security-password` variable with `nvrnm` because the password is visible when viewing the environment variable list. The `nvrnm` tool requires system administrator or root access to set environment variables.

To securely set the password for EFI, use the Firmware Password Utility.

### From the Command Line:

```
# Securing Global System Settings
# -----
# Configuring Open Firmware Settings
# -----
# Secure startup by setting security-mode. Replace $mode-value with
# "command" or "full".
nvram security-mode="$mode-value"
# Verify security-mode setting.
nvram -p
```

## Intel-Based Macintosh Systems

Macintosh computers with Intel processors use EFI to control low-level hardware. EFI is similar to BIOS on an x86 PC and is the hardware base layer for Mac OS X computers with Intel processors. By protecting it from unauthorized access you can prevent attackers from gaining access to your computer.



Intel-based and PowerPC-based computers can use the Firmware Password Utility to password protect the hardware layer. For information on using the Firmware Password Utility, see “Using the Firmware Password Utility” on page 54.

## Configuring Access Warnings

You can use a login window or Terminal access warning to provide notice of a computer’s ownership, to warn against unauthorized access, or to remind authorized users of their consent to monitoring.

### Enabling Access Warnings for the Login Window

Before enabling an access warning, review your organization’s policy for what to use as an access warning.

When a user tries to access the computer’s login window (locally or through Apple Remote Desktop), the user sees the access warning you create, such as the following:



#### To create a login window access warning:

- 1 Open Terminal and verify that your logged-in account can use `sudo` to perform a `defaults write`.
- 2 Change your login window access warning:  

```
$ sudo defaults write /Library/Preferences/com.apple.loginwindow  
LoginwindowText "Warning Text"
```

Replace *Warning Text* with your access warning text.
- 3 Log out to test your changes.  
Your access warning text appears below the Mac OS X subtitle.

## From the Command Line:

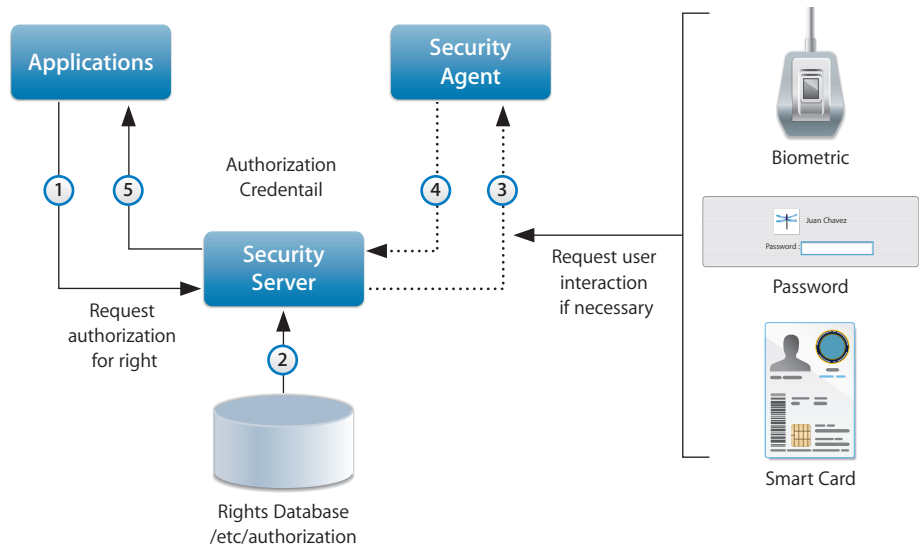
```
# Enabling Access Warning for the Login Window
# -----
# Create a login window access warning.
defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText
    "Warning Text"
# You can also used the BannerSample project to create an access warning.
```

## Understanding the AuthPlugin Architecture

AuthPlugins are used to control access to a service or application. Preinstalled AuthPlugins for Mac OS X are located in the `/System/Library/CoreServices/SecuritiyAgentPlugins/` folder. These plug-ins (along with their associated rules and authorization rights for users) are defined in the `/etc/authorization` database, and are queried by the Security Server.

For more information about `/etc/authorization`, see “Managing Authorization Through Rights” on page 209.

The following graphic shows the workflow of the Security Server.



When an application requests authorization rights from the security server the security server interrogates the rights database (/etc/authorization) to determine the mechanisms to be used for authentication. If necessary, the security server requests user interaction through the security agent. The security agent then prompts the user to authenticate through the use of a password, biometric, or Smart Card device. Then the security agent sends the authentication information back to the security server, which passes it back to the application.

## Understanding the BannerSample Project

If your computer has developer tools installed, the sample code for the banner sample project is located in /Developer/examples/security/bannersample. You can modify and customize this sample banner code for your organization. After you compile the code you can place it in the /Library/Security/SecurityAgentPlugins/ folder. Then modify the key `system.login.console` in the /etc/authorization file using Terminal.

For more information about the banner sample, see the bannersample README file.

**To modify the /etc/authorization file:**

- 1 Open Terminal.
- 2 Enter the following command:  

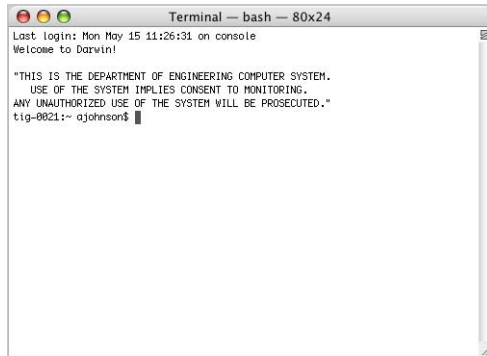
```
$ sudo pico /etc/authorization
```
- 3 Locate the `system.login.console` key.
- 4 Add `<string>bannersample:test</string>` above `<string> builtin:smartcard-siffer,privileged</string>`, as shown in bold below:  

```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>comment</key>
<string>Login mechanism based rule. Not for general use, yet.</string>
<key>mechanisms</key>
<array>
  <string>bannersample:test</string>
  <string>builtin:smartcard-sniffer,privileged</string>
```
- 5 Save changes and exit the editor.
- 6 Restart the computer and verify that the banner appears.

## Enabling Access Warnings for the Command Line

Before enabling an access warning, review your organization's policy for what to use as an access warning.

When a user opens Terminal locally or connects to the computer remotely, the user sees the access warning you create. The following task must be performed by an administrator user. You can use any text editor.



**To create a command-line access warning:**

- 1 Open Terminal.
- 2 Enter the following command to create the `/etc/motd` file:  

```
$ sudo touch /etc/motd
```
- 3 Enter the following command to edit the `/etc/motd` file:  

```
$ sudo pico /etc/motd
```
- 4 Enter in your access warning message.
- 5 Save changes and exit the text editor.
- 6 Open a new Terminal window to test changes.

Your access warning text appears above the prompt in the new Terminal window.

Use this chapter to learn how to secure accounts by assigning user account types, configuring directory access, using strong authentication procedures, and by safely storing credentials.

Securing user accounts requires determining how accounts are used and setting the level of access for users.

When you define a user’s account you specify the information to prove the user’s identity, such as user name, authentication method (password, digital token, smart card, or biometric reader), and user identification number (user ID). Other information in a user’s account is needed by various services—to determine what the user is authorized to do and to personalize the user’s environment.

Types of User Accounts

When you log in to Mac OS X, you use a nonadministrator or administrator account. The main difference is that Mac OS X provides safety mechanisms to prevent nonadministrator users from editing key preferences, or from performing actions critical to computer security. Administrator users are not as limited as nonadministrator users.

You can further define nonadministrator and administrator accounts by specifying additional user privileges or restrictions.

The following table shows the access provided to user accounts.

User Account	User Access
Guest nonadministrator	Restricted user access (disabled by default)
Standard nonadministrator	Nonprivileged user access
Managed nonadministrator	Restricted user access
Administrator	Full computer configuration administration
System administrator (root)	Unrestricted access to the computer

Unless you need administrator access for specific system maintenance tasks that cannot be accomplished by authenticating with the administrator's account while logged in as a normal user, always log in as a nonadministrator user. Log out of the administrator account when you are not using the computer as an administrator. Never browse the web or check email while logged in to an administrator's account.

If you are logged in as an administrator, you are granted privileges and abilities that you might not need. For example, you can potentially modify system preferences without being required to authenticate. This authentication bypasses a security safeguard that prevents malicious or accidental modification of system preferences.

## Guidelines for Creating Accounts

When you create user accounts, follow these guidelines:

- Never create accounts that are shared by several users. Each user should have his or her own standard or managed account.

Individual accounts are necessary to maintain accountability. System logs can track activities for each user account, but if several users share the same account it is difficult to track which user performed an activity. Similarly, if several administrators share a single administrator account, it becomes harder to track which administrator performed an action.

If someone compromises a shared account, it is less likely to be noticed. Users might mistake malicious actions performed by an intruder for legitimate actions by a user sharing the account.

- Each user needing administrator access should have an administrator account in addition to a standard or managed account.

Administrator users should only use their administrator accounts for administrator purposes. By requiring an administrator to have a personal account for typical use and an administrator account for administrator purposes, you reduce the risk of an administrator performing actions like accidentally reconfiguring secure system preferences.

## Defining User IDs

A user ID is a number that uniquely identifies a user. Mac OS X computers use the user ID to track a user's folder and file ownership. When a user creates a folder or file, the user ID is stored as the creator ID. A user with that user ID has read and write permissions to the folder or file by default.

The user ID is a unique string of digits between 500 and 2,147,483,648. New users created using the Accounts pane of System Preferences are assigned user IDs starting at 501.

It is risky to assign the same user ID to different users, because two users with the same user ID have identical directory and POSIX file permissions. However, each user has a unique GUID that is generated when the user account is created. Your GUID is associated with ACL permissions that are set on files or folders. By setting ACL permissions you can prevent users with identical user IDs from accessing files and folders.

The user ID 0 is reserved for the root user. User IDs below 100 are reserved for system use; user accounts with these user IDs should not be deleted and should not be modified except to change the password of the root user.

If you don't want the user name to appear in the login window of a computer, assign a user ID of less than 500 and enter the following command in a Terminal window:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow Hide500Users  
-bool YES
```

In general, after a user ID is assigned and the user starts creating files and folders, you shouldn't change the user ID.

One possible scenario in which you might need to change a user ID is when merging users from different servers onto a new server or cluster of servers. The same user ID might have been associated with a different user on the previous server.

## Securing the Guest Account

The guest account is used to give a user temporary access to your computer. The guest account should be disabled by default because it does not require a password to log in on the computer. If this account is enabled and is not securely configured, malicious users can gain access to your computer without the use of a password.

In security sensitive environments the guest account should remain disabled. If you do enable the guest account, enable parental controls to limit what the user can do. Whether or not the guest account itself is enabled, disable guest account access to shared files and folders by deselecting the "Allow guest to connect to shared folders" checkbox. If you permit the guest account to access shared folders, an attacker can easily attempt to access shared folders without a password.

When you finish with this account, disable it by deselecting the "Allow guests to log into this computer." This prevents the guest user account from logging into the computer.

For more information about parental controls, see "Controlling Local Accounts with Parental Controls" on page 64.

## Securing Nonadministrator Accounts

There are two types of nonadministrator user accounts:

- Standard user accounts, which don't have administrator privileges and don't have parental controls limiting their actions.
- Managed user accounts, which don't have administrator privileges, but have active parental controls. Parental controls help deter unsophisticated users from performing malicious activities. They can also help prevent users from misusing their computer.

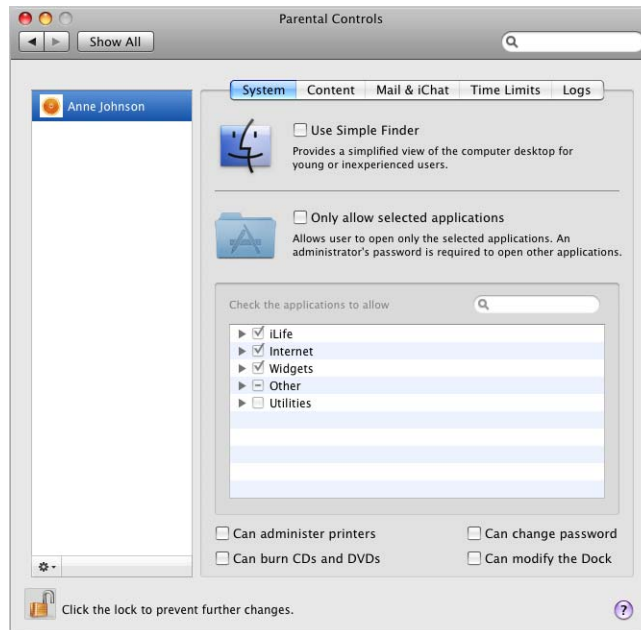
**Note:** If your computer is connected to a network, a managed user can also be a user whose preferences and account information are managed through the network.

When creating nonadministrator accounts, restrict the accounts so they can only use what is required. For example, if you plan to store sensitive data on your local computer, disable the ability to burn DVDs.

## Controlling Local Accounts with Parental Controls

You can set limits for users by using Parental Controls preferences. For example, you might want to prevent users from being able to install or uninstall software, or you might want to restrict access to specific administrator tools or utilities. The preferences can be set according to your environment.

The following screen shows Parental Controls that you can set to restrict accounts.





**To securely configure an account with parental controls:**

- 1 Open System Preferences, then click Accounts.
- 2 If the lock icon is locked, click the lock icon and enter an administrator name and password.
- 3 Select the user account you want to manage with parental controls and select the Enable Parental Controls checkbox.
- 4 Click Open Parental Controls.
- 5 Click System.

You can enable Simple Finder, which restricts an account to using applications listed on the Dock. With Simple Finder enabled, users can't create or delete files. Simple Finder also prevents users from changing their passwords.

Enabling Simple Finder is not recommended, unless your computer is used in a kiosk-like environment.

In the System pane you can specify the applications the user has access to by selecting the "Only allow selected applications" checkbox. Then you can select or deselect applications in the applications list.

When you install third-party applications, you can add them to this list. Disable third-party applications unless the user needs to use such an application and can do so in a secure manner. Third-party applications might give a standard user some administrator abilities, which can be a security issue.

You can also prevent the user from administering printers, changing his or her password, burning CDs and DVDs, and modifying the Dock by deselecting associated checkboxes.

- 6 Click Content.

In the Content pane you can restrict the websites that users can view by selecting "Try to limit access to adult websites automatically" and you can customize the list of adult sites by clicking customize and adding the URL of sites to the "Always allow these sites" list or the "Never allow these sites" list.

You can also select Allow access to only these websites, which prevents a user from accessing any site not in the list. The list can be expanded by clicking the Add (+) button below the list of sites.

- 7 Click Mail & iChat.

In the Mail & iChat pane you can limit Mail and iChat to specific mail and iChat addresses in the "Only allow emailing and instant messaging with" list. To add users to the list, click the Add (+) button below the list.

You can also require that mail addressed to a recipient not listed must have permission to be sent by selecting the “Send permission request to” checkbox and entering an administrator’s mail address. When a user attempts to send mail, the mail is sent to the administrator’s mail address for permission to be sent.

#### 8 Click Time Limits.

In the Time Limits pane you can restrict the number of hours the computer is used during Monday through Friday or weekends by selecting the “Limit computer use to” checkbox and setting the number of hours.

You can also set the times the computer can be accessed by selecting “weekday Sunday through Thursday” or “weekends Friday and Saturday,” and setting a time range.

#### 9 Click Logs.

In the Logs pane you can view a user’s activity on the web or a specific application, from the current day to an entire year. If you see an activity you want to prevent a user from using, select the activity and then click Restrict.

### Securing External Accounts

An external account is a mobile account that has its local home folder stored on a volume in an external drive. When an external account logs in, Mac OS X only shows the external account that the user logged in with. The external user account cannot view other accounts on the computer.

External accounts require Mac OS X version 10.5 Leopard or later and an external or ejectable volume that is formatted as Mac OS X Extended format (HFS Plus). If you use an external account use FileVault to protect the content of your home folder in case your external volume is stolen or lost.

For information about external accounts, see *User Management*.

### Protecting Data on External Volumes

By default a user’s home folder is not encrypted. If a user stores their home folder on an external volume using an external account, the user must secure the data on the external volume. To secure the external volume:

- The volume must be able to process an external authentication, such as a PIN or smart card before it is mounted or readable.
- The user’s home folder should use FileVault or other encryption mechanisms to secure the data.

## Securing Directory-Based Accounts

Directory-based account is an account is located on a directory server. A directory server contains user account records and important data for authenticating users. If your computer is connected to a directory server, you can add directory users to your computer and grant them access. You can restrict a directory user account by using Parental Controls.

Access to directory servers is usually tightly restricted to protect the data on them.

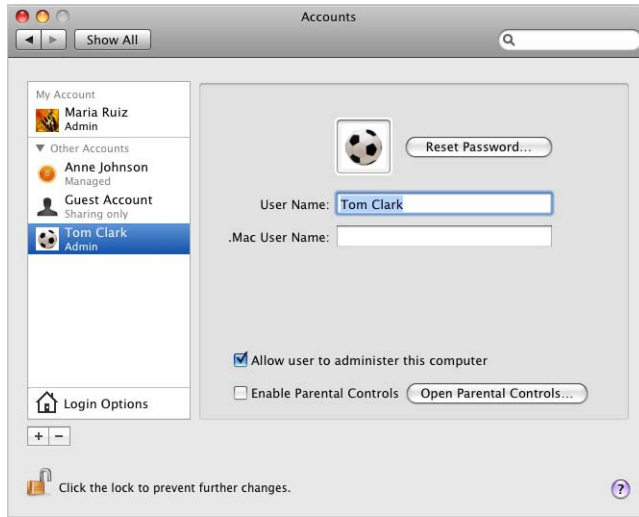
## Securing Administrator Accounts

Each administrator should have two accounts: a standard account for daily use and an administrator account for administrator access. Remember that the non-administrative account should be used for most daily activity, especially when accessing the network or Internet. The administrator's account should be use only when absolutely necessary to accomplish administrative tasks. To secure administrator accounts, restrict the distribution of administrator accounts and limit the use of these accounts.

A user account with administrator privileges can perform standard user and administrator tasks such as:

- Creating user accounts
- Adding users to the Admin group
- Changing the FileVault master password
- Enabling or disabling sharing
- Enabling, disabling, or changing firewall settings
- Changing other protected areas in System Preferences
- Installing system software

The following screen shows an account enabled to be an administrator account.



## Securing the System Administrator Account

The most powerful user account in Mac OS X is the system administrator or root account. By default, the root account on Mac OS X is disabled and it is recommended you do not enable it. The root account is primarily used for performing UNIX commands. Generally, actions that involve critical system files require you to perform those actions as root.

If you are logged in as a Mac OS X administrator, you perform commands as root or by using the `sudo` command. Mac OS X logs actions performed using the `sudo` command. This helps you track misuse of the `sudo` command on a computer.

You can use the `su` command to log in to the command line as another user. By entering `su root`, you can log in as the root user (if the root account is enabled). You can use `sudo` to perform commands that require root privileges. You should restrict access to the root account.

If multiple users can log in as root, you cannot track which user performed root actions.

Do not allow direct root login because the logs cannot identify which administrator logged in. Instead, log in using accounts with administrator privileges, and then use the `sudo` command to perform actions as root.

For instructions about how to restrict root user access in Directory Utility, open Mac Help and search for "Directory Utility."

You can also disable the root account by using an administrative account and the `dsenableroot` command. For example, the following command disables the root account.

```
$ dsenableroot -d
```

By default, `sudo` is enabled for administrator users. From the command line, you can disable root login or restrict the use of `sudo`. Limit the administrators allowed to use `sudo` to those who require the ability to run commands as root.

The computer uses a file named `/etc/sudoers` to determine which users can use `sudo`. You can modify root user access by changing the `/etc/sudoers` file to restrict `sudo` access to specific accounts, and allow those accounts to perform specifically allowed commands. This gives you control over what users can do as root.

**To restrict sudo usage, change the `/etc/sudoers` file:**

- 1 As the root user, use the following command to edit the `/etc/sudoers` file, which allows for safe editing of the file.

```
$ sudo visudo
```

- 2 When prompted, enter the administrator password.

There is a timeout value associated with `sudo`. This value indicates the number of minutes until `sudo` prompts for a password again. The default value is 5, which means that after issuing the `sudo` command and entering the correct password, additional `sudo` commands can be entered for 5 minutes without reentering the password.

This value is set in the `/etc/sudoers` file. For more information, see the `sudo` and `sudoers` man pages.

- 3 In the Defaults specification section of the file, add the following lines.

```
Defaults timestamp_timeout=0
Defaults tty_tickets
```

These lines limit the use of the `sudo` command to a single command per authentication and also ensure that, even if a timeout is activated, that later `sudo` commands are limited to the terminal in which authentication occurred.

- 4 Restrict which administrators can run `sudo` by removing the line that begins with `%admin`, and add the following entry for each user, substituting the user's short name for the word *user*:

```
user ALL=(ALL) ALL
```

Doing this means that when an administrator is added to the computer, the administrator must be added to the `/etc/sudoers` file as described, if the administrator needs to use `sudo`.

- 5 Save and quit `visudo`.

For more information, enter `man vi` or `man visudo` in a Terminal window. For information about how to modify the `/etc/sudoers` file, see the `sudoers` man page.

## Understanding Directory Domains

User accounts are stored in a directory domain. Your preferences and account attributes are set according to the information stored in the directory domain.

Local accounts are hosted in a local directory domain. When you log in to a local account, you authenticate with that local directory domain. Users with local accounts typically have local home folders. When a user saves files in a local home folder, the files are stored locally. To save a file over the network, the user must connect to the network and upload the file.

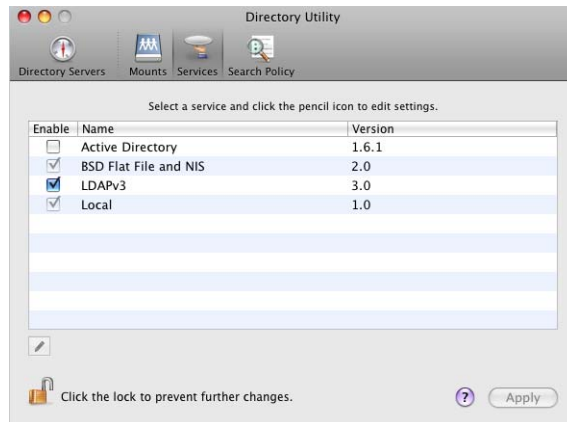
Network-based accounts are hosted in a network-based directory domain, such as a Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) directory. When you log in to a network-based account, you authenticate with the network-based directory domain. Users with network accounts typically have network home folders. When they save files in their network home folders, the files are stored on the server.

Mobile accounts cache authentication information and managed preferences. A user's authentication information is maintained on the directory server but is cached on the local computer. With cached authentication information, a user can log in using the same user name and password (or a digital token, smart card, or biometric reader), even if the user is not connected to the network.

Users with mobile accounts have local and network home folders which combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders. For information about protecting your home folder, see Chapter 7, "Securing Data and Using Encryption," on page 129.

## Understanding Network Services, Authentication, and Contacts

You can use Directory Utility to configure your computer to use a network-based directory domain. Disable directory search services that are not used by deselecting them in the Services pane of Directory Utility (shown here).



You can enable or disable each kind of directory service protocol in Directory Utility.

Mac OS X doesn't access disabled directory services, except for the local directory domain, which is always accessed.

In addition to enabling and disabling services, you can use Directory Utility to choose the directory domains you want to authenticate with. Directory Utility defines the authentication search policy that Mac OS X uses to locate and retrieve user authentication information and other administrative data from directory domains.

The login window Finder and other parts of Mac OS X use this authentication information and administrative data. File service, Mail service, and other services provided by Mac OS X Server also use this information.

Directory Utility also defines the contacts search policy that Mac OS X uses to locate and retrieve name, address, and other contact information from directory domains. Address Book can use this contact information, and other applications can be programmed to use it as well.

The authentication and contacts search policy consists of a list of directory domains (also known as directory nodes). The order of directory domains in the list defines the search policy.

Starting at the top of the list, Mac OS X searches each listed directory domain in turn until it finds the information it needs or reaches the end of the list without finding the information.

For more information about using Directory Utility, see *Open Directory Administration*.

## Configuring LDAPv3 Access

Mac OS X Leopard primarily uses Open Directory as its network-based directory domain. Open Directory uses LDAPv3 as its connection protocol. LDAPv3 includes several security features that you should enable if your server supports them. Enabling every LDAPv3 security feature maximizes LDAPv3 security.

To make sure your settings match your network's required settings, contact your network administrator. Whenever possible, all LDAP connections should be configured to be encrypted using SSL.

When configuring LDAPv3, do not add DHCP-supplied LDAP servers to automatic search policies if you cannot secure the network the computer is running on. If you do, someone can create a rogue DHCP server and a rogue LDAP directory and then control your computer as the root user.

For information about changing the security policy for an LDAP connection or for information about protecting computers from malicious DHCP servers, see *Open Directory Administration*.

## Configuring Active Directory Access

Mac OS X Leopard supports mutual authentication with Active Directory servers. Kerberos is a ticket-based system that enables mutual authentication. The server must identify itself by providing a ticket to your computer. This prevents your computer from connecting to rogue servers.

Mac OS X Leopard also supports digital signing and encrypted packet security settings used by Active Directory. These settings are enabled by default.

Mutual authentication occurs when you bind to Active Directory servers.

If you're connecting to an Active Directory server with Highly Secure (HISEC) templates enabled, you can use third-party tools to further secure your Active Directory connection.

When you configure Active Directory access, the settings you choose are generally dictated by the Active Directory server's settings. To make sure your settings match your network's required settings, contact your network administrator.

The "Allow administration by" setting should not be used in sensitive environments. It can cause unintended privilege escalation issues because any member of the group specified will have administrator privileges on your computer. Additionally, you should only connect to trusted networks.



For more information about using Directory Utility to connect to Active Directory servers, see *Open Directory Administration*.

## Using Strong Authentication

Authentication is the process of verifying the identity of a user. Mac OS X supports local and network-based authentication to ensure that only users with valid authentication credentials can access the computer's data, applications, and network services.

You can require passwords to log in, to wake the computer from sleep or from a screen saver, to install applications, or to change system settings. Mac OS X also supports authentication methods such as smart cards, digital tokens, and biometric readers.

Strong authentication is created by using combinations of the following authentication dimensions:

- What the user knows, such as a password or PIN number
- What the user has, such as one-time-password (OTP) token or smart card
- What the user is, such as a fingerprint, retina scan, or DNA sample

Using a combination of these dimensions makes authentication more reliable and user identification more certain.

## Using Password Assistant to Generate or Analyze Passwords

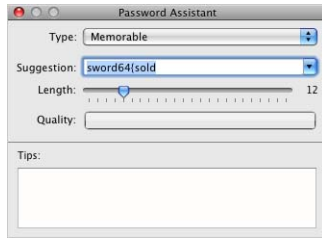
Mac OS X includes Password Assistant, an application that analyzes the complexity of a password or generates a complex password for you. You can specify the length and type of password you'd like to generate.

You can choose from the following types of passwords:

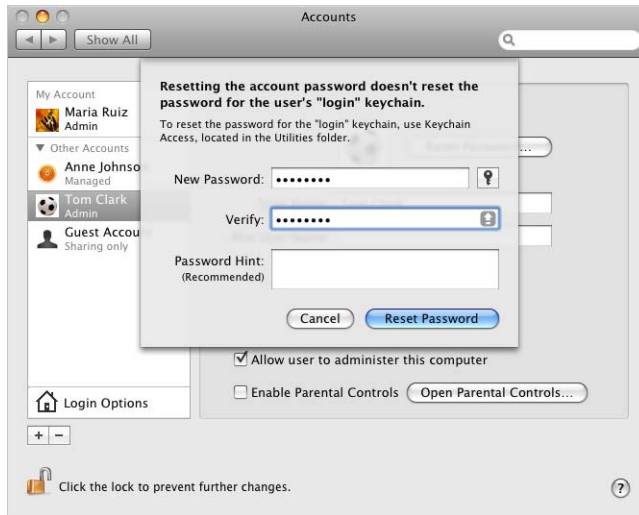
- **Manual:** You enter a password and then Password Assistant gives you the quality level of your password. If the quality level is low, Password Assistant gives tips for increasing the quality level.
- **Memorable:** According to your password length requirements, Password Assistant generates a list of memorable passwords in the Suggestion menu.
- **Letters & Numbers:** According to your password length requirements, Password Assistant generates a list of passwords with a combination of letters and numbers.
- **Numbers Only:** According to your password length requirements, Password Assistant generates a list of passwords containing only numbers.
- **Random:** According to your password length requirements, Password Assistant generates a list of passwords containing random characters.
- **FIPS-181 compliant:** According to your password length requirements, Password Assistant generates a password that is FIPS-181 compliant (which includes mixed upper and lowercase, punctuation, and numbers).

For example, you can create a randomly generated password or a FIPS-181 compliant password that is 12 characters long.

The following screen shows Password Assistant.



You can open Password Assistant from some applications. For example, when you create an account or change passwords in Accounts preferences, you can use Password Assistant to help you create a secure password.



## Using Kerberos

Kerberos is an authentication protocol used for systemwide single sign-on, allowing users to authenticate to multiple services without reentering passwords or sending them over the network. Every system generates its own principals, allowing it to offer secure services that are fully compatible with other Kerberos-based implementations.

**Note:** Mac OS X Leopard support Kerberos v5 but does not support Kerberos v4.

Mac OS X Leopard uses Kerberos to make it easier to share services with other computers. A key distribution center (KDC) server is not required to use Kerberos authentication between two Mac OS X Leopard computers.

When you connect to a computer that supports Kerberos, you are granted a ticket that permits you to continue to use services on that computer, without reauthentication, until your ticket expires.

For example, consider two Mac OS X 10.5 computers named "Mac01" and "Mac02." Mac02 has screen sharing and file sharing turned on. If Mac01 connects to a shared folder on Mac02, Mac01 can subsequently connect to screen sharing on Mac02 without needing to supply login credentials again.

This Kerberos exchange is only attempted if you connect using Bonjour, if you navigate to the computer in Finder, or if you use the Go menu in Finder to connect to a server using the local hostname of the computer name (for example, *computer\_name.local*).

Kerberos is also used to secure the Back to My Mac (BTMM) service. For more information about using Kerberos with BTMM, see "Securing BTMM Access" on page 188.

Normally, after your computer gains a Kerberos ticket in this manner, keep the Kerberos ticket until it expires. However, if you want to manually remove your Kerberos ticket, you can do so using the Kerberos utility in Mac OS X.

**To manually remove a Kerberos ticket:**

- 1 Open Keychain Access (in /Applications/Utilities).
- 2 From the Keychain Access menu, choose Kerberos Ticket Viewer.
- 3 In the Kerberos application's Ticket Cache window, find the key that looks like this:  
`"yourusername@LKDC:SHA1..."`  
It is followed by a long string of alphanumeric characters.
- 4 Click "Destroy" to delete that key.

You can also use the `kinit`, `kdestroy`, and `kpasswd` commands to manage Kerberos tickets. For more information, see `kinit`, `kdestroy`, and `kpasswd` man pages.

## Using Smart Cards

A smart card is a plastic card (similar in size to a credit card) or USB dongle that has memory and a microprocessor embedded in it. The smart card can store and process information such as passwords, certificates, and keys.

The microprocessor inside the smart card can do authentication evaluation offline before releasing information.

Before the smart card processes information, you must authenticate with the smart card by a PIN or biometric measurement (such as a fingerprint), which provides an additional layer of security.

Smart card support is integrated into Mac OS X Leopard and can be configured to work with the following services:

- Cryptographic login (local or network based accounts)
- Unlock of FileVault enabled accounts
- Unlock keychains
- Signed and encrypted email (S/MIME)
- Securing web access (HTTPS)
- VPN (L2TP, PPTP, SSL)
- 802.1X
- Screen saver unlock
- System administration
- Keychain Access

For more information, see the *Smart Card Setup Guide* at [www.apple.com/server/macosx/resources/](http://www.apple.com/server/macosx/resources/).

## Using Tokens

You can use a digital token to identify a user for commerce, communication, or access control. This token can be generated by software or hardware.

Some common tokens are the RSA SecurID and the CRYPTOCARD KT-1 devices. These hardware devices generate tokens to identify the user. The generated tokens are specific to that user, so two users with different RSA SecurIDs or different CRYPTOCARD KT-1s have different tokens.

You can use tokens for two-factor authentication. *Two-factor* refers to authenticating through something you have (such as a one-time-password token) and something you know (such as a fixed password). The use of tokens increases the strength of the authentication. Tokens are frequently used for VPN authentication.

## Using Biometrics

Mac OS X supports biometrics authentication technologies such as thumbprint readers. Password-protected websites and applications can be accessed without requiring the user to remember a long list of passwords.

Some biometric devices allow you to authenticate by placing your finger on a pad. Unlike a password, your fingerprint can never be forgotten or stolen. Fingerprint identification provides personal authentication and network access.

The use of biometrics can add an additional factor to authentication by using something that is a part of you (such as your fingerprint).

## Setting Global Password Policies

To configure a password policy that can apply globally or to individual users, use the `pwdpolicy` command-line tool.

Global password policies are not implemented in Mac OS X; instead, password policies are set for each user account.

You can set specific rules governing the size and complexity of acceptable passwords. For example, you can specify requirements for the following:

- Minimum and maximum character length
- Alphabetic and numeric character inclusion
- Maximum number of failed logins before account lockout

To require that an authenticator's password be a minimum of 12 characters and have no more than 3 failed login attempts, enter the following in a Terminal window:

```
$ pwdpolicy -n /Local/Default -setglobalpolicy "minChars=12  
maxFailedLoginAttempts=3"
```

For advanced password policies, use Password Server in Mac OS X Server. You can use it to set global password policies that specify requirements for the following:

- Password expiration duration
- Special character inclusion
- Mixed-case character inclusion
- Password reuse limits

You can use `pwdpolicy` to set a password policy that meets your organization's password standards. For more information about how to use `pwdpolicy`, enter `man pwdpolicy` in a Terminal window.

## Storing Credentials

Mac OS X includes Keychain Access, an application that manages collections of passwords and certificates in a single credential store called a keychain. Each keychain can hold a collection of credentials and protect them with a single password.

Keychains store encrypted passwords, certificates, and other private values (called secure notes). These values are accessible only by unlocking the keychain using the keychain password and only by applications that are approved and added to the access control application list.

You can create multiple keychains, each of which appears in a keychain list in Keychain Access. Each keychain can store multiple values. Each value is called a key item. You can create a key item in any user-created keychain.

When an application must store an item in a keychain, it stores it in the keychain designated as your default. The default is named “login,” but you can change that to any user-created keychain. The default keychain name is displayed in bold.

Each item in a keychain has an Access Control List (ACL) that can be populated with applications that have authority to use that keychain item. A further restriction can be added that forces an application with access to confirm the keychain password.

The main issue with remembering passwords is that you’re likely to make all passwords identical or keep a written list of passwords. By using keychains, you can greatly reduce the number of passwords you need to remember. Because you no longer need to remember passwords for multiple accounts, the passwords you choose can be very complex and can even be randomly generated.

Keychains provide additional protection for passwords, passphrases, certificates, and other credentials stored on the computer. In some cases, such as using a certificate to sign a mail message, the certificate must be stored in a keychain.

If a credential must be stored on the computer, store and manage it using Keychain Access. Check your organization’s policy on keychain use.

Due to the sensitive nature of keychain information, keychains use cryptography to encrypt and decrypt secrets, and they safely store secrets and related data in files.

Mac OS X Keychain services enable you to create keychains and provide secure storage of keychain items. After a keychain is created, you can add, delete, and edit keychain items, such as passwords, keys, certificates, and notes. A user can unlock a keychain with a single password and applications can then use that keychain to store and retrieve data, such as passwords.

## Using the Default User Keychain

When a user’s account is created, a default keychain named “login” is created for that user. The password for the login keychain is initially set to the user’s login password and is unlocked when the user logs in. It remains unlocked unless the user locks it, or until the user logs out.

You should change the settings for the login keychain so the user must unlock it when he or she logs in, or after waking the computer from sleep.

### To secure the login keychain:

- 1 Open Keychain Access.
- 2 If you do not see a list of keychains, click Show Keychains.
- 3 Select the login keychain.
- 4 Choose Edit > Change Password for Keychain “login.”
- 5 Enter the current password, and create and verify a password for the login keychain.

After you create a login keychain password that is different from the normal login password, your keychain is not unlocked at login.

To help you create a more secure password, use Password Assistant. For information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.

- 6 Choose Edit > Change Settings for Keychain “login.”
- 7 Select “Lock when sleeping.”
- 8 Deselect “Synchronize this keychain using MobileMe.”
- 9 Secure each login keychain item.

For information, see “Securing Keychains and Their Items” on page 80.

## Creating Additional Keychains

When a user account is created it contains only the initial default keychain named “login.” A user can create additional keychains, each of which can have different settings and purposes.

For example, a user might want to group credentials for mail accounts into one keychain. Because mail programs query the server frequently to check for mail, it is not practical for the user to reauthenticate when such a check is performed.

The user could create a keychain and configure its settings, so that he or she is required to enter the keychain password at login and whenever the computer is awakened from sleep.

He or she could then move all items containing credentials for mail applications into that keychain and set each item so that only the mail application associated with that credential can automatically access it. This forces other applications to authenticate to access that credential.

Configuring a keychain’s settings for use by mail applications might be unacceptable for other applications. If a user has an infrequently used web-based account, it is more appropriate to store keychain settings in a keychain configured to require reauthentication for every access by any application.

You can also create multiple keychains to accommodate varying degrees of sensitivity. By separating keychains based on sensitivity, you prevent the exposure of sensitive credentials to less sensitive applications with credentials on the same keychain.

### To create a keychain and customize its authentication settings:

- 1 In Keychain Access, choose File > New Keychain.
- 2 Enter a name, select a location for the keychain, and click Create.
- 3 Enter a password, verify it, and click OK.
- 4 If you do not see a list of keychains, click Show Keychains.

- 5 Select the new keychain.
- 6 Choose Edit > Change Settings for keychain "*keychain\_name*," and authenticate, if requested.
- 7 Change the "Lock after # minutes of inactivity" setting based on the access frequency of the security credentials included in the keychain.

If the security credentials are accessed frequently, do not select "Lock after # minutes of inactivity."

If the security credentials are accessed frequently, select "Lock after # minutes of inactivity" and select a value, such as 15. If you use a password-protected screensaver, consider setting this value to the idle time required for your screensaver to start.

If the security credentials are accessed infrequently, select "Lock after # minutes of inactivity" and specify a value, such as 1.
- 8 Select "Lock when sleeping."
- 9 Drag the security credentials from other keychains to the new keychain and authenticate, if requested.

You should have keychains that only contain related certificates. For example, you could have a mail keychain that only contains mail items.
- 10 If you are asked to confirm access to the keychain, enter the keychain password and click Allow Once.

After confirming access, Keychain Access moves the security credential to the new keychain.
- 11 Secure each item in the security credentials for your keychain.

You can also use the `security` and `systemkeychain` commands to create and manage your keychains. For more information, see the `security` and `systemkeychain man` pages. For information, see "Securing Keychains and Their Items" on page 80.

## Securing Keychains and Their Items

Keychains can store multiple encrypted items. You can configure items so only specific applications have access. (However, you cannot set Access Control for certificates.)

### To secure a keychain item:

- 1 In Keychain Access, select a keychain and then select an item.
  - 2 Click the Information (i) button.
  - 3 Click Access Control and then authenticate if requested.
  - 4 Select "Confirm before allowing access."
- After you enable this option, Mac OS X prompts you before giving a security credential to an application.



If you selected “Allow all applications to access this item” you allow any application to access the security credential when the keychain is unlocked. When accessing the security credential, there is no user prompt, so enabling this is a security risk.

**5** Select “Ask for Keychain password.”

After enabling this, you must provide the keychain password before applications can access security credentials.

Enabling this is important for critical items, such as your personal identity (your public key certificates and the corresponding private key), which are needed when signing or decrypting information. These items can also be placed in their own keychains.

**6** Remove nontrusted applications listed in “Always allow access by these applications” by selecting each application and clicking the Remove (–) button.

Applications listed here require the user to enter the keychain password to access security credentials.

## Using Smart Cards as Keychains

Mac OS X Leopard integrates support for hardware-based smart cards as dynamic keychains where any application using keychains can access that smart card. A smart card can be thought of as a portable protected keychain.

Smart cards are seen by the operating system as dynamic keychains and are added to the top of the Keychain Access list. They are the first searched in the list. They can be treated as other keychains on the user’s computer, with the limitation that users can’t add other secure objects.

When you attach a supported smart card to your computer, it appears in Keychain Access. If multiple smart cards are attached to your computer, they will appear at the top of the keychain list alphabetically as separate keychains.

You can manually unlock and change the PIN using Keychain Access. When changing the PIN on your smart card it is the same as changing the password on a regular keychain.

In Keychain Access, select your smart card and unlock it by double-clicking it. If it is not unlocked, you are prompted to enter the password for the smart card, which is the same as the PIN. Enter the PIN and Keychain Access will bring up the PIN-protected data on that smart card.

For more information, see the *Smart Card Setup Guide* at [www.apple.com/server/macosx/resources/](http://www.apple.com/server/macosx/resources/).

## Using Portable and Network-Based Keychains

If you're using a portable computer, consider storing your keychains on a portable drive, such as a USB flash memory drive. You can remove the portable drive from the portable computer and store it separately when the keychains are not in use.

Anyone attempting to access data on the portable computer needs the portable computer, portable drive, and password for the keychain stored on the portable drive. This provides an extra layer of protection if the laptop is stolen or misplaced.

To use a portable drive to store keychains, move your keychain files to the portable drive and configure Keychain Access to use the keychains on the portable drive.

The default location for your keychain is ~/Library/Keychains/. However, you can store keychains in other locations.

You can further protect portable keychains by storing them on biometric USB flash memory drives, or by storing portable drive contents in an encrypted file. For information, see "Encrypting Portable Files" on page 143.

Check with your organization to see if they allow portable drives to store keychains.

### To set up a keychain for use from a portable drive:

- 1 Open Keychain Access.
- 2 If you do not see a list of keychains, click Show Keychains.
- 3 Choose Edit > Keychain List.
- 4 Note the location of the keychain you want to set up.  
The default location is ~/Library/Keychains/.
- 5 Click Cancel.
- 6 Select the keychain you want set up.
- 7 Choose File > Delete Keychain "*keychain\_name*."
- 8 Click Delete References.
- 9 Copy the keychain files from the previously noted location to the portable drive.
- 10 Move the keychain to the Trash and use Secure Empty Trash to securely erase the keychain file stored on the computer.  
For information, see "Using Secure Empty Trash" on page 148.
- 11 Open Finder and double-click the keychain file on your portable drive to add it to your keychain search list.

## About Certificates

A certificate is a piece of cryptographic information that enables the safe transfer of information over the Internet. Certificates are used by web browsers, mail applications, and online chat applications.

When you communicate with a secure site, the information exchanged with the site is encrypted. This protects your login information, credit card numbers, addresses, and other secure data.

In Mac OS X, certificates are part of your digital identity and are stored in your keychain. Keychain Access lets you manage your certificates and keychains.

Certificates are issued by trusted organizations, such as VeriSign, Inc. or RSA Data Security, Inc. When you go to a secure website, Mac OS X checks the site's certificate and compares it with certificates that are known to be legitimate. If the website's certificate is not recognized, or if the site doesn't have one, you receive a message.

The validity of a certificate is verified electronically using the public key infrastructure, or PKI. Certificates consist of your public key, the identity of the organization, the certificate authority (CA) that signed your certificate, along with other data that may be associated with your identity.

A certificate is usually restricted for particular uses, such as digital signatures, encryption, use with web servers, and so on. This is called the "key use" restriction. While it's possible to create one certificate for multiple uses, it's unusual to make one for all possible uses. Creating a certificate for multiple uses is also less secure.

A certificate is valid only for a limited time; it then becomes invalid and must be replaced with a newer version. The certificate authority can also revoke a certificate before it expires.

If you need to send a certificate to someone, you can export it using Keychain Access, and then send it through email or by other means. Likewise, if someone sends you a certificate, you can add it to your keychain by dragging it onto the Keychain Access icon, or by using the Import menu in Keychain Access.

## Creating a Self-signed Certificate

You can create a certificate using the Certificate Assistant in Keychain Access. The certificate you create is called a self-signed certificate. Self-signed certificates don't provide the guarantees of a certificate signed by a certificate authority.

### To create a self-signed certificate:

- 1 Open Keychain Access, located in the Utilities folder in the Applications folder.
- 2 Choose Keychain Access > Certificate Assistant > "Create a Certificate."
- 3 Enter a name for the certificate, choose a type, and then click Continue.

- **Self-signed root certificate:** A self-signed root certificate is a root certificate authority that someone makes for immediate use as a certificate. Such certificates do not benefit from the security of certificate chains and certificate policies. Most computers do not accept a self-signed certificate unless their owner first tells them to, and some computers do not accept them under any circumstances. They are however easy and quick to make, and are often used for testing purposes in place of certificates signed by proper certificate authorities.
  - **Leaf certificate:** A leaf is a certificate signed by an intermediate or root Certificate Authority. A leaf certificate benefits from the security of certificate chains and certificate policies. A leaf is situated at the bottom of a certificate chain.
- 4 Select “Let me override defaults” if you want to manually specify the information in the certificate, such as key pairs, extensions, and encryption.
  - 5 Review the certificate and click Done.

## Adding Certificates to a Keychain

Digital certificates are used to validate users and hosts on the Internet. When you receive certificates from the Internet, you can add them to your keychain for quick access to secure websites and other resources. Once a certificate is added, it can be used by other compatible applications.

### To add a certificate to a keychain:

- 1 Drag the certificate file onto the Keychain Access icon or double-click the certificate file.
- 2 If you want to view the contents of the certificate before you add it, click View Certificates in the dialog, and then click OK when you are done.
- 3 Choose a keychain from the pop-up menu and click OK.
- 4 If you’re asked to provide a name and password, type the name and password for an administrator user on this computer.

For Keychain Access to recognize a certificate file, it must have a file extension that identifies it as containing certificates.

The following types of certificates are recognized by Keychain Access:

- PKCS12 DER encoded - extension .p12 or .pfx
- PKCS7 DER or PEM encoded - extension .p7r, .p7b, .p7m, .p7c, or .p7s

If Keychain Access is open, you can add a certificate by dragging the certificate onto the Keychain Access icon in the Dock.

You can also add a certificate to a keychain by choosing File > Import in Keychain Access.

Use this chapter to set Mac OS X system preferences to customize system security and further protect against attacks.

System Preferences has many configurable preferences that you can use to customize system security.

## System Preferences Overview

Mac OS X includes system preferences that you can use to customize security. When modifying settings for one account, make sure your settings are mirrored on all other accounts, unless there is an explicit need for different settings.

You can view system preferences by choosing Apple > System Preferences. In the System Preferences window, click a preference to view it.

The following is the System Preferences screen:



Some critical preferences require that you authenticate before you modify their settings. To authenticate, you click the lock (see the images below) and enter an administrator's name and password (or use a digital token, smart card, or biometric reader).



If you log in as a user with administrator privileges, these preferences are unlocked unless you select "Require password to unlock each System Preferences pane" in Security preferences. For more information, see "Securing Security Preferences" on page 112.

If you log in as a standard user these preferences remain locked. After unlocking preferences, you can lock them again by clicking the lock.

Preferences that require authentication include the following:

- Accounts
- Date & Time
- Energy Saver
- Network
- Parental Controls
- Print & Fax
- Security
- Sharing
- Startup Disk
- Time Machine

This chapter lists each set of preferences included with Mac OS X and describes modifications recommended to improve security.

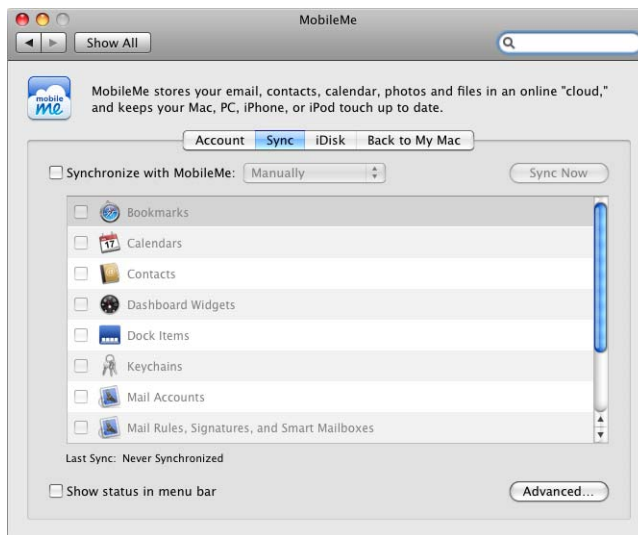
## Securing MobileMe Preferences

MobileMe is a suite of Internet tools that help you synchronize data and other important information when you're away from the computer.

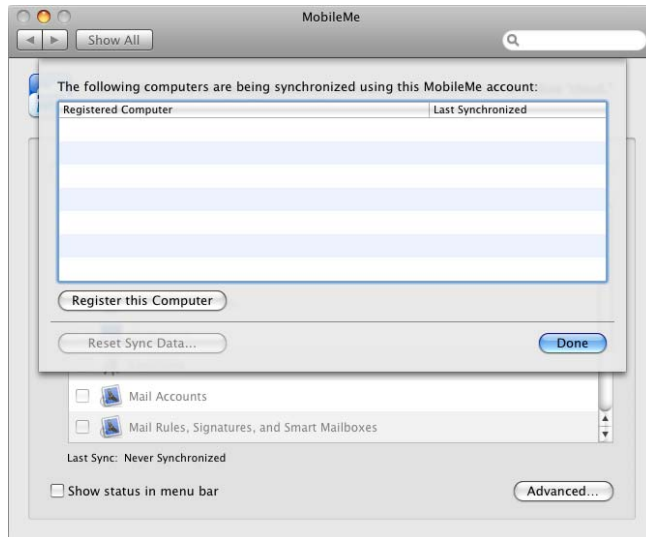
In sensitive environments don't use MobileMe. If you must store critical data, only store it on your local computer. You should only transfer data over a secure network connection to a secure internal server.

If you use MobileMe, enable it only for user accounts that don't have access to critical data. It is not recommended that you enable MobileMe for administrator or root user accounts.

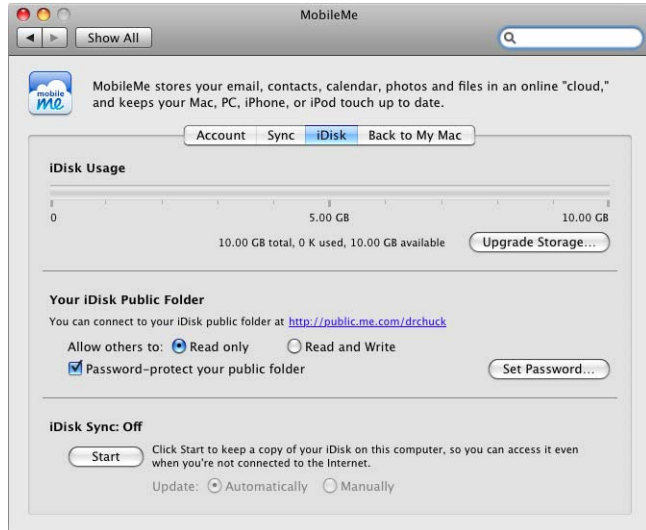
Leave the options disabled in the Sync pane of MobileMe preferences (shown below).



Leave Registered Computer for synchronization blank in the Advanced settings of the Sync pane (shown below).



Leave iDisk Syncing (shown below) disabled by default. If you must use a Public folder, enable password protection.



**To disable MobileMe preferences:**

- 1 Open MobileMe preferences.
- 2 Deselect "Synchronize with MobileMe."



- 3 Make sure there are no computers registered for synchronization in the Advanced settings of the Sync pane.
- 4 Make sure iDisk Syncing is disabled in the iDisk pane.

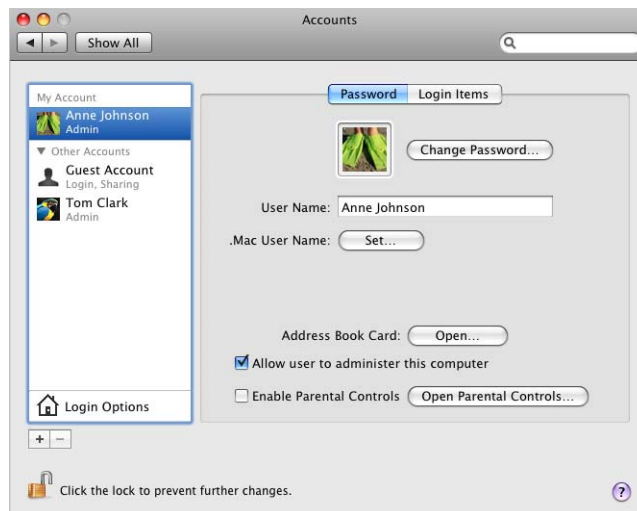
#### From the Command Line:

```
# -----  
# Securing System Preferences  
# -----  
# Securing MobileMe Preferences  
# -----  
# Disable Sync options.  
defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer 1  
# Disable iDisk Syncing.  
defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool no
```

## Securing Accounts Preferences

Use Accounts preferences to change or reset account passwords (shown below), to enable Parental Controls, or to modify login options for each account.

You should immediately change the password of the first account that was created on your computer. If you are an administrator, you can change other user account passwords by selecting the account and clicking Change Password.



**Note:** If you are an administrator, password policies are not enforced when you change your password or when you change another user's password. Therefore, when you are changing passwords as an administrator, make sure you follow the password policy that you set. For more information about password policies, see “Setting Global Password Policies” on page 77.

The password change dialog (shown below) and the reset dialog provide access to Password Assistant, an application that can analyze the strength of your password and assist you in creating a more secure password. For information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.



Consider the following login guidelines:

- Modify login options to provide as little information as possible to the user.
- Require that the user know which account they want to log in with and the password for that account.
- Disable automatic login if enabled.
- Require that the user enter a name and a password, and that the user authenticate without the use of a password hint.
- Disable fast user switching if enabled—it is a security risk because it allows multiple users to be simultaneously logged in to a computer.

You should also modify login options to disable the Restart, Sleep, and Shut Down buttons. By disabling these buttons, the user cannot restart the computer without pressing the power key or logging in.

**To securely configure Accounts preferences:**

- 1 Open Accounts preferences.
- 2 Select an account and click the Password tab; then, change the password by clicking the Change Password button.

A menu appears asking you to input the old password, new password, verification of the new password, and a password hint.

- 3 Do not enter a password hint, then click the Change Password button.
- 4 Click Login Options.

A screen similar to the following appears:



- 5 Under "Display login window as," select "Name and password" and deselect all other options.

## From the Command Line:

```
# Securing Accounts Preferences
# -----
# Change an account's password.
# Don't use the following command on a computer that could possibly have
# other users logged in simultaneously.
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass
# Make sure there is no password hint set.
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint
    -int 0
# Set the login options to display name and password in the login window.
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -
    bool yes
# Disable Show the Restart, Sleep, and ShutDown Buttons.
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
    bool yes
# Disable fast user switching.
defaults write /Library/Preferences/.GlobalPreferences
    MultipleSessionEnabled -bool NO
```

## Securing Appearance Preferences

One method to secure appearance preferences is to change the number of recent items displayed in the Apple menu to None.

Recent items are applications, documents, and servers you've recently used. You access recent items by choosing Apple > Recent Items.

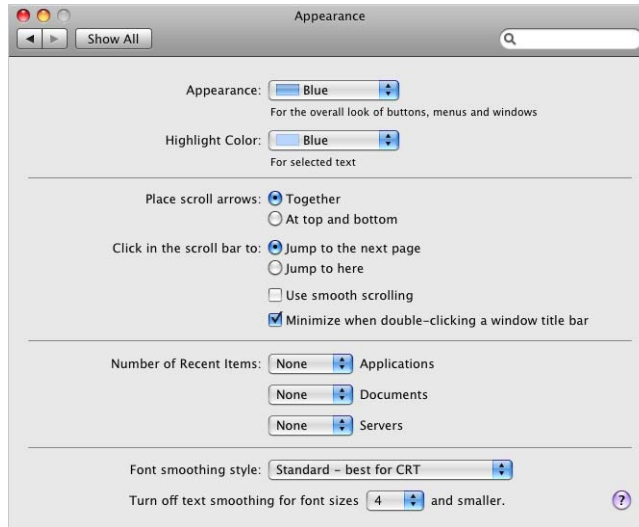
If intruders gain access to your computer, they can use recent items to quickly view your most recently accessed files. Additionally, intruders can use recent items to access authentication mechanisms for servers if the corresponding keychains are unlocked.

Removing recent items provides a minimal increase in security, but it can deter unsophisticated intruders.

## To securely configure Appearance preferences:

- 1 Open Appearance preferences.

A screen similar to the following appears:



- 2 Set all “Number of Recent Items” preferences to None.

### From the Command Line:

```
# Securing Appearance Preferences
# -----
# Disable display of recent applications.
defaults write com.apple.recentitems Applications -dict MaxAmount 0
```

## Securing Bluetooth Preferences

Bluetooth allows wireless devices, such as keyboards, mice, and mobile phones, to communicate with the computer. If the computer has Bluetooth capability, Bluetooth preferences become available. If you don't see Bluetooth preferences, you cannot use Bluetooth.

**Note:** Some high security areas do not allow radio frequency (RF) communication such as Bluetooth. Consult your organizational requirements for possible further disablement of the component.

When you disable Bluetooth in System Preferences, you must disable Bluetooth for every user account on the computer.

This does not prevent users from reenabling Bluetooth. You can restrict a user account's privileges so the user cannot reenabling Bluetooth, but to do this, you remove several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 61.

**To securely configure Bluetooth preferences:**

- 1 Open Bluetooth preferences.

A screen similar to the following appears:



- 2 Deselect "Bluetooth Power."

**From the Command Line:**

```
# Securing Bluetooth Preferences
# -----
# Turn Bluetooth off.
defaults write /Library/Preferences/com.apple.Bluetooth \
    ControllerPowerState -int 0
```

## Securing CDs & DVDs Preferences

To secure CDs and DVDs, do not allow the computer to perform automatic actions when the user inserts a disc.

When you disable automatic actions in System Preferences, you must disable these actions for every user account on the computer.

This does not prevent users from reenabling automatic actions. To prevent the user from reenabling automatic actions, you must restrict the user's account so the user cannot open System Preferences. For more information on restricting accounts, see "Securing Nonadministrator Accounts" on page 64.

### To securely configure CDs & DVDs preferences:

- 1 Open CDs & DVDs preferences.

A screen similar to the following appears:



- 2 Disable automatic actions when inserting media by choosing Ignore for each pop-up menu.

### From the Command Line:

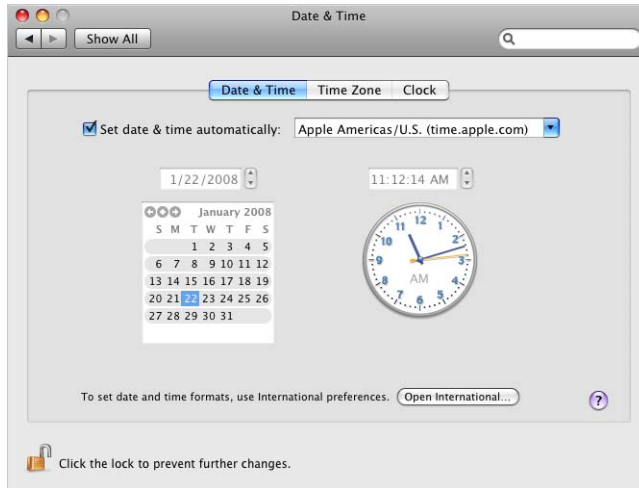
```
# Securing CDs & DVDs Preferences
# -----
# Disable blank CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.cd.appeared -dict action 1
# Disable music CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.music.appeared -dict action 1
# Disable picture CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.picture.appeared -dict action 1
# Disable blank DVD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.dvd.appeared -dict action 1
# Disable video DVD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.dvd.video.appeared -dict action 1
```

## Securing Date & Time Preferences

Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues.

You can use Date & Time preferences (shown below) to set the date and time based on a Network Time Protocol (NTP) server.

If you require automatic date and time, use a trusted, internal NTP server.



**To securely configure Date & Time preferences:**

- 1 Open Date & Time preferences.
- 2 In the Date & Time pane, enter a secure and trusted NTP server in the “Set date & time automatically” field.
- 3 Click the Time Zone button.

A screen similar to the following appears:





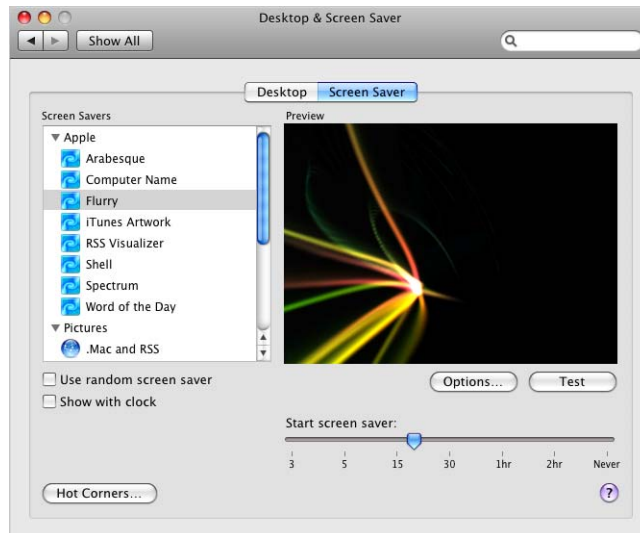
#### 4 Choose a time zone.

##### From the Command Line:

```
# Securing Date & Time Preferences
# -----
# Set the NTP server.
cat >> /etc/ntp.conf << END server time.apple.com END
# Set the date and time.
systemsetup -settimezone $Time_Zone
```

## Securing Desktop & Screen Saver Preferences

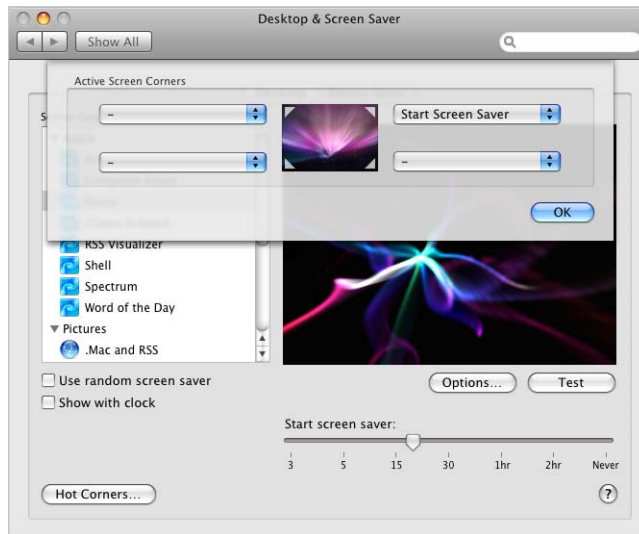
You can use Desktop & Screen Saver preferences (shown below) to configure a password-protected screen saver to prevent unauthorized users from accessing unattended computers.



You can use several authentication methods to unlock the screen saver, including digital tokens, smart cards, and biometric readers.

You should also set a short inactivity interval to decrease the amount of time the unattended computer is unlocked. For information about requiring authentication for screen savers, see “Securing Security Preferences” on page 112.

You can configure Desktop & Screen Saver preferences to allow you to quickly enable or disable screen savers if you move your mouse cursor to a corner of the screen, as shown below. (You can also do this by configuring Exposé & Spaces preferences.)



When you configure Desktop & Screen Saver preferences, you configure the preferences for every user account on the computer.

This doesn't prevent users from reconfiguring their preferences. You can restrict a user's account privileges so the user cannot reconfigure preferences. Doing this removes several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 61.

**To securely configure Desktop & Screen Saver preferences:**

- 1 Open Desktop & Screen Saver preferences.
  - 2 Click the Screen Saver pane.
  - 3 Set "Start screen saver" to a short inactivity time.
  - 4 Click Hot Corners.
  - 5 Set a corner to Start Screen Saver for quick enabling of the screen saver.
- Don't set a screen corner to disable Screen Saver.

## From the Command Line:

```
# Securing Desktop & Screen Saver Preferences
# -----
# Set idle time for screen saver. XX is the idle time in seconds.
defaults -currentHost write com.apple.screensaver idleTime -int XX
# Set host corner to activate screen saver.
#wvous-bl-corner (bottom-left)
#wvous-br-corner (bottom-right)
#wvous-tl-corner (top-left)
#wvous-tr-corner (top-right)
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-corner
-int 5
# Set modifier key to 0 wvous-corner_code-modifier
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
modifier -int 0
```

## Securing Display Preferences

If multiple displays are attached to your computer, enabling display mirroring might expose private data to others. Having this additional display provides extra opportunity for others to see private data.

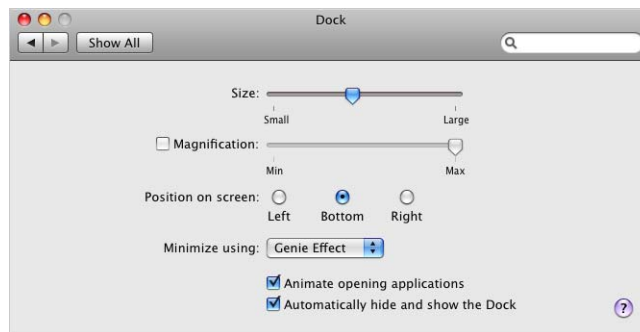
## Securing Dock Preferences

You can configure the Dock to be hidden when not in use, which can prevent others from seeing the applications you have on your computer.

### To securely configure Dock preferences:

- 1 Open Dock preferences.

The following screen appears:



- 2 Select "Automatically hide and show the Dock."

## From the Command Line:

```
# Securing Dock Preferences
# -----
# Automatically hide and show Dock.
defaults write /Library/Preferences/com.apple.dock autohide -bool YES
```

## Securing Energy Saver Preferences

You can use the Energy Saver Sleep pane (shown in the procedure below) to configure a period of inactivity before a computer, display, or hard disk enters sleep mode.

If the computer receives directory services from a network that manages its client computers and your computer is in sleep mode, it is unmanaged and cannot be detected as being connected to the network. To allow management and network visibility, configure the display and the hard disk to sleep, but not the computer.

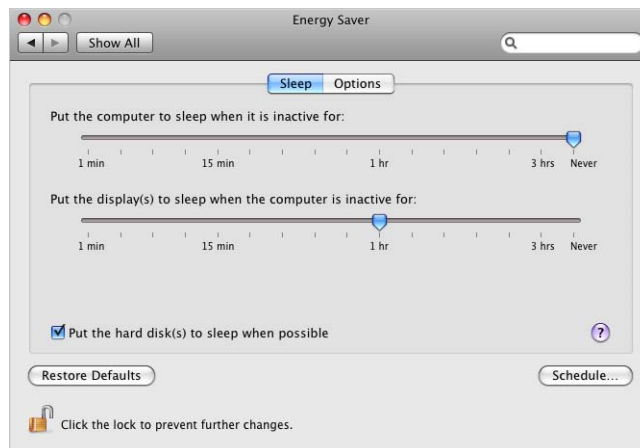
You can require authentication by use of a password, digital token, smart card, or biometric reader to reactivate the computer (see “Securing Security Preferences” on page 112). This is similar to using a password-protected screen saver.

You can also use the Options pane to make settings depending on your power supply (power adapter, UPS, or battery). Configure the computer so it only wakes when you physically access the computer. Also, don't set the computer to restart after a power failure.

### To securely configure Energy Saver preferences:

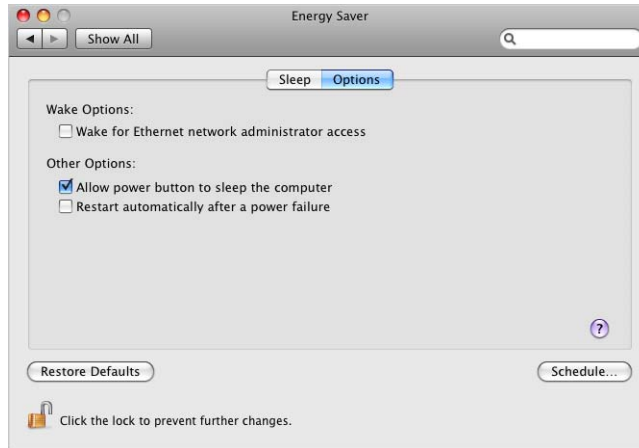
- 1 Open Energy Saver preferences.

A screen similar to the following appears:



- 2 From the Sleep pane, set “Put the computer to sleep when it is inactive for” to Never.
- 3 Select “Put the hard disk(s) to sleep when possible” and then click the “Options” pane.

A screen similar to the following appears:



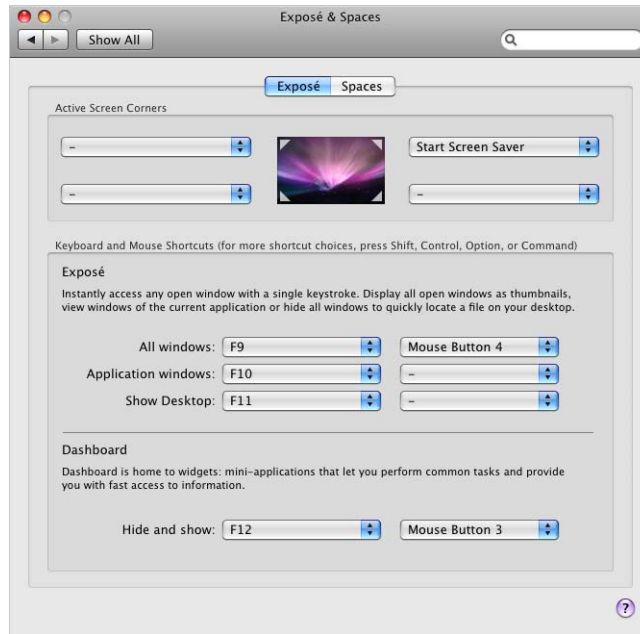
- 4 Deselect “Wake for Ethernet network administrator access” and “Restart automatically after a power failure.”

#### From the Command Line:

```
# Securing Energy Saver Preferences
# -----
# Disable computer sleep.
pmset -a sleep 0
# Enable hard disk sleep.
pmset -a disksleep 1
# Disable Wake for Ethernet network administrator access.
pmset -a womp 0
# Disable Restart automatically after power failure.
pmset -a autorestart 0
```

## Securing Exposé & Spaces Preferences

Your computer should require authentication when waking from sleep or screen saver. You can configure Exposé & Spaces preferences (shown below) to allow you to quickly start the screen saver if you move your mouse cursor to a corner of the screen. Don't configure a corner to disable the screen saver.



For information about requiring authentication for the screen saver, see “Securing Security Preferences” on page 112.

Dashboard widgets included with Mac OS X can be trusted. However, be careful when you install third-party Dashboard widgets. You can install Dashboard widgets without authenticating. To prevent Dashboard from running remove the Dashboard application from the /Applications folder.

When you configure Exposé & Spaces preferences, you must configure these preferences for every user account on the computer.

This doesn't prevent users from reconfiguring their preferences. You can restrict a user account's privileges so the user cannot reconfigure preferences. To do this, you remove several important user abilities, like the user's ability to change his or her password. For more information, see “Types of User Accounts” on page 61.

If your organization does not want to use Dashboard because of its potential security risk, you can disable it. If the user has access to the Terminal application, Dashboard can be re-enabled at any time.

Dashboard uses the `com.apple.dashboard.fetch` service to fetch updates to widgets from the Internet. If Dashboard is disabled, this service should be disabled as well. This service must be disabled from the command line, using the command shown in the instructions below.

#### From the Command Line:

```
# Securing Exposé & Spaces Preferences
# -----
# Disable dashboard.
$ sudo launchctl unload -w /System/Library/LaunchDaemons/
    com.apple.dashboard.advisory.fetch.plist
```

## Securing International Preferences

No security-related configuration is necessary. However, if your computer uses more than one language, review the security risk of the language character set. Consider deselecting unused packages during Mac OS X installation.

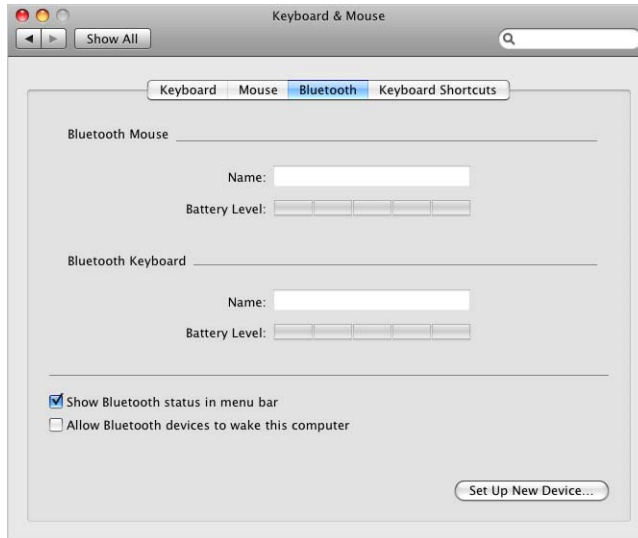
## Securing Keyboard & Mouse Preferences

If Bluetooth is not required, turn it off. If Bluetooth is necessary, disable allowing Bluetooth devices to awake the computer.

#### To securely configure Keyboard & Mouse preferences:

- 1 Open Keyboard & Mouse preferences.
- 2 Click Bluetooth.

A screen similar to the following appears.



- 3 Deselect “Allow Bluetooth devices to wake this computer.”

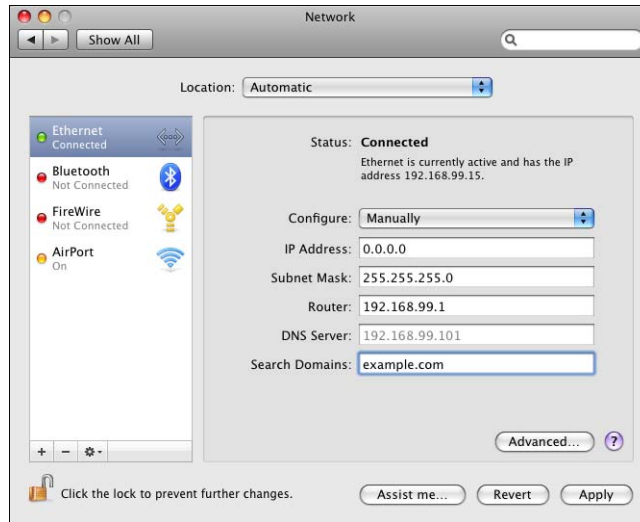
**From the Command Line:**

```
# Securing Keyboard & Mouse Preferences
# -----
# Disable Bluetooth Devices to wake computer.
defaults write /Library/Preferences/com.apple.Bluetooth \
    BluetoothSystemWakeEnable -bool 0
```



## Securing Network Preferences

It is recommended that you disable unused hardware devices listed in Network preferences (shown below). Enabled, unused devices (such as AirPort and Bluetooth) are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.



When configuring your computer for network access, use a static IP address when possible. A DHCP IP address should be used only if necessary.

Some organizations use IPv6, a new version of the Internet protocol (IP). The primary advantage of IPv6 is that it increases the address size from 32 bits (the current IPv4 standard) to 128 bits.

An address size of 128 bits is large enough to support a large number of addresses. This allows more addresses or nodes than are otherwise available. IPv6 also provides more ways to set up the address and simplifies autoconfiguration.

By default IPv6 is configured automatically, and the default settings are sufficient for most computers that use IPv6. You can also configure IPv6 manually. If your organization's network cannot use or does not require IPv6, turn it off.

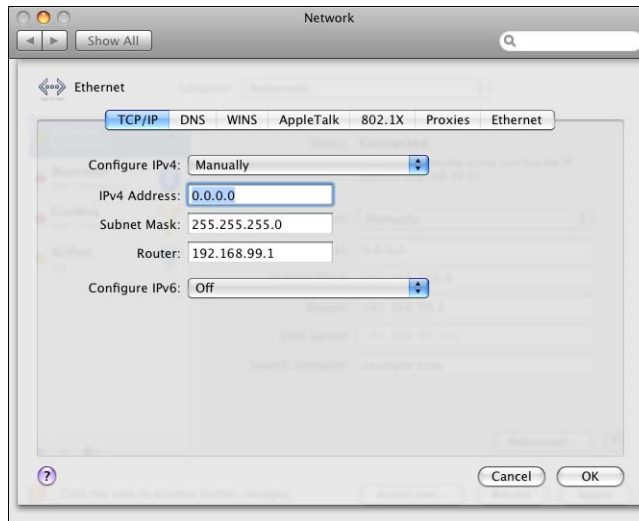
### To securely configure Network preferences:

- 1 Open Network preferences.
- 2 From the list of hardware devices, select the hardware device you use to connect to your network (For example, AirPort or Ethernet).
- 3 From the Configure pop-up menu, choose Manually.

Enter your static IP address, Subnet Mask, Router, DNS Server, and Search Domain configuration settings.

4 Click Advanced.

A screen similar to the following appears:



5 In the Configure IPv6 pop-up menu, choose Off.

If you frequently switch between AirPort and Ethernet, you can disable IPv6 for AirPort and Ethernet or any hardware device that you use to connect to your network.

6 Click OK.

**From the Command Line:**

```
# Securing Network Preferences
# -----
# Disable IPv6.
# The interface value can be AirPort, Bluetooth, Ethernet, or FireWire.
networksetup -setv6off $interface
```

## Securing Parental Controls Preferences

Parental Controls enable you to customize access controls for each account. You must set Parental Controls for each account. You cannot enable Parental Controls for the administrator account logged in to the computer at that time.

Use the following System pane options to limit access to applications and other functions:

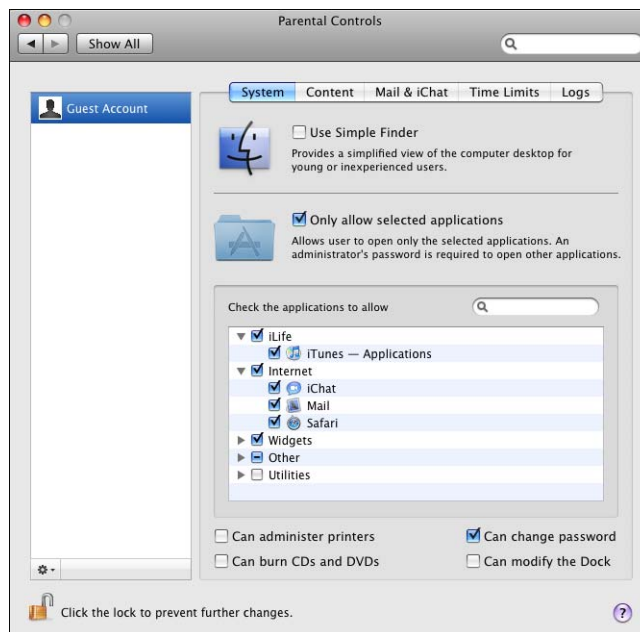
- Only allow selected applications. You can restrict the user's access to specific applications by deselecting the checkbox next to the application in the "Check the applications to allow" list.
- Can administer printers. You can restrict the user's ability to select alternative printers and to change printer settings.
- Can burn CDs and DVDs. You can limit the user's ability to burn CDs and DVDs on the computer.
- Can change password. Users should always have the ability to change their password.
- Can modify the Dock. You can limit the user's ability to add or remove applications from the Dock.

In the Content pane, use the "Allow access to only these websites" option to restrict and define a list of approved websites that the user can visit.

### To secure Parental Controls preferences:

- 1 Open Parental Controls preferences.

A screen similar to the following appears:

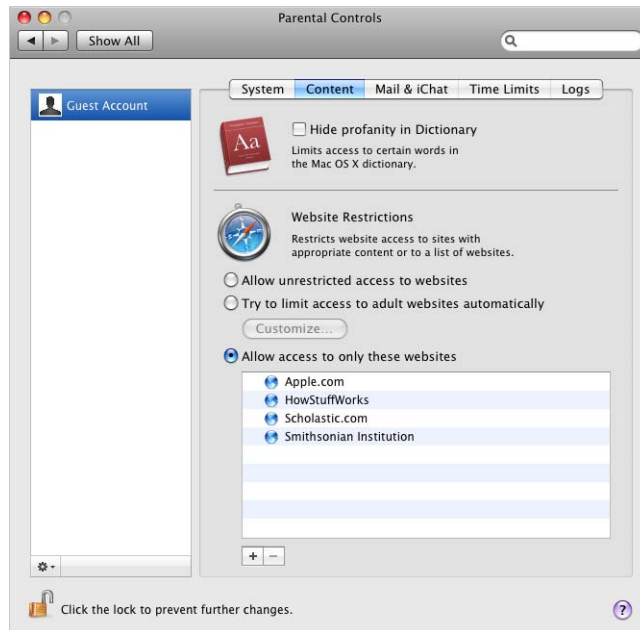


- 2 Select the account you want to activate parental controls for.

If the account you want to manage is not listed, open Account preferences and click the lock to authenticate, if it is locked. From the accounts list, select the account you want to manage. Then select the “Enable Parental Control” checkbox and click Open Parental Controls.

- 3 In the System pane, enable “Only allow selected applications” to restrict application access to specific applications.
- 4 From “Check the applications to allow” select the applications that the user can access.
- 5 Disable the following other features that the user should not perform:
  - Can administer printers
  - Can burn CDs and DVDs
  - Can modify the dock
- 6 Select the Content pane.

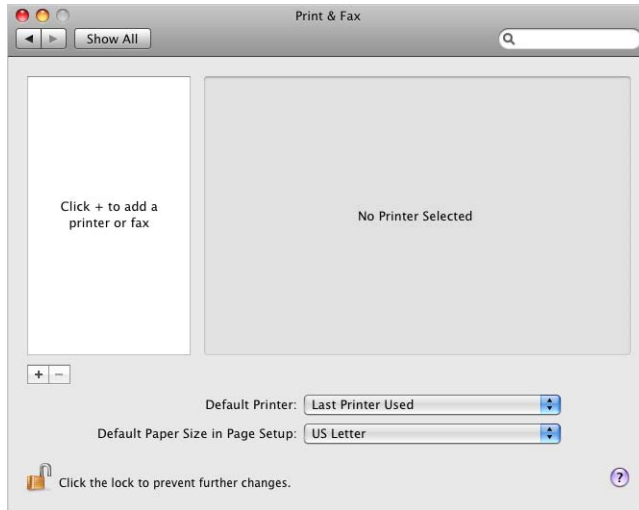
A screen similar to the following appears:



- 7 In the Content pane, limit website access to specific sites by selecting “Allow access to only these websites.”
- 8 Select “Add bookmark” from the pop-up menu and enter the website name and address.

## Securing Print & Fax Preferences

The Print & Fax preferences screen looks like this:



Only use printers in a secure location. If you print confidential material in an insecure location, the material might be viewed by unauthorized users.

Be careful when printing to a shared printer. Doing so allows other computers to capture the print job directly. Another computer could be maliciously monitoring and capturing confidential data being sent to the real printer. In addition, unauthorized users can add items to your print queue without authenticating.

You can access your printer using the CUPS web interface (<http://localhost:631>). The CUPS web interface by default cannot be accessed remotely. It can only be accessed by the local host.

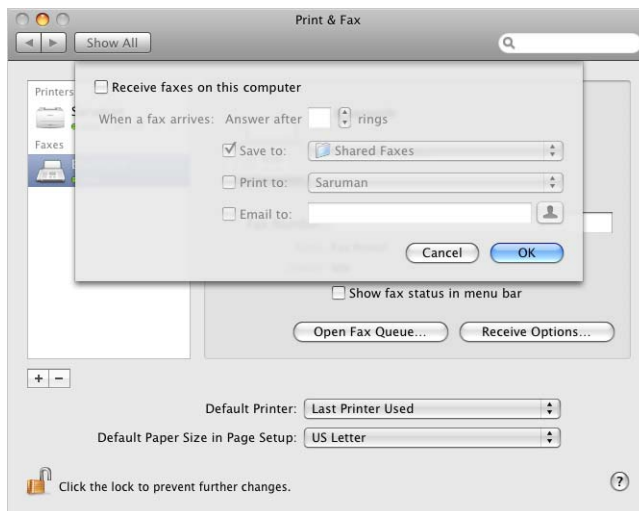
You can create policies in CUPS that restrict users from such actions as canceling jobs or deleting printers using the CUPS web interface. For more information about creating CUPS policies, see <http://localhost:631/help/policies.html>.

To avoid an additional avenue of attack, don't receive faxes on your computer.

**To securely configure Print & Fax preferences:**

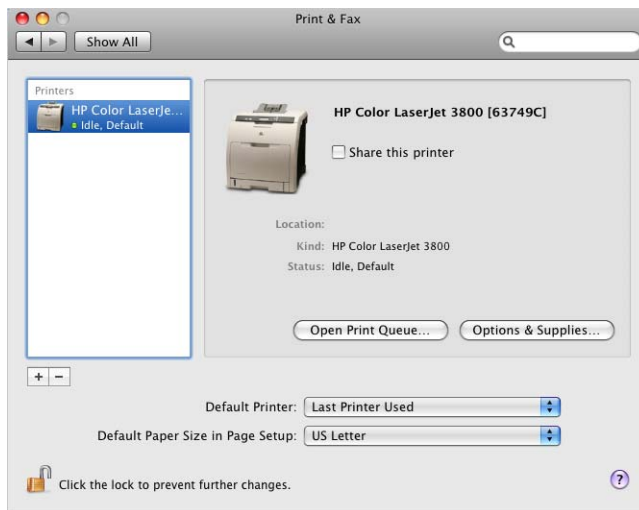
- 1 Open Print & Fax preferences and select a fax from the equipment list.
- 2 Click Receive Options.

A screen similar to the following appears:



- 3 Deselect "Receive faxes on this computer."
- 4 Click OK.
- 5 Select a printer from the equipment list.

A screen similar to the following appears:



## 6 Deselect “Share this printer.”

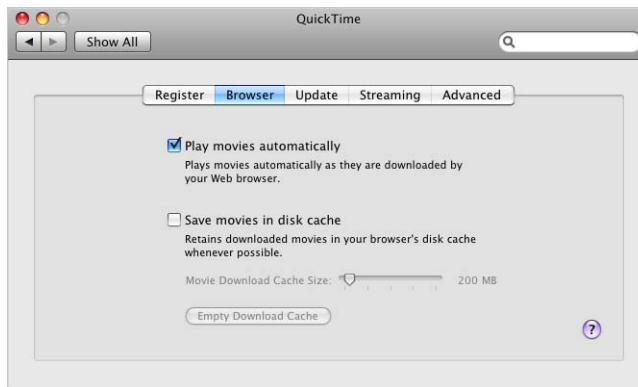
### From the Command Line:

```
# Securing Printer & Fax Preferences
# -----
# Disable the receiving of faxes.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist
# Disable printer sharing.
cp /etc/cups/cupsd.conf $TEMP_FILE
if /usr/bin/grep "Port 631" /etc/cups/cupsd.conf
then
    usr/bin/sed "/^Port 631.*s//Listen localhost:631/g" $TEMP_FILE
    > /etc/cups/cupsd.conf
else
echo "Printer Sharing not on"
fi
```

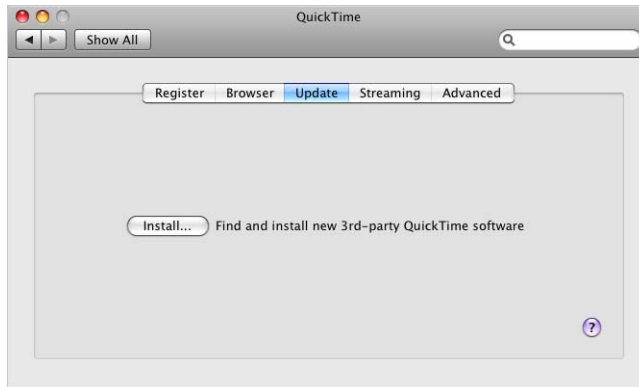
## Securing QuickTime Preferences

Only download QuickTime movies from trusted, secure sources. By default, QuickTime stores downloaded movies in a cache. If someone gains access to your account they can see your previously viewed movies, even if you did not save them as files.

You can change QuickTime preferences to disable the storing of movies in a cache (in */Users/user name/Library/Caches/QuickTime/downloads/*), as shown here.



You can find and install third-party QuickTime software using the Update pane. Install third-party QuickTime software only if your organization requires that software.

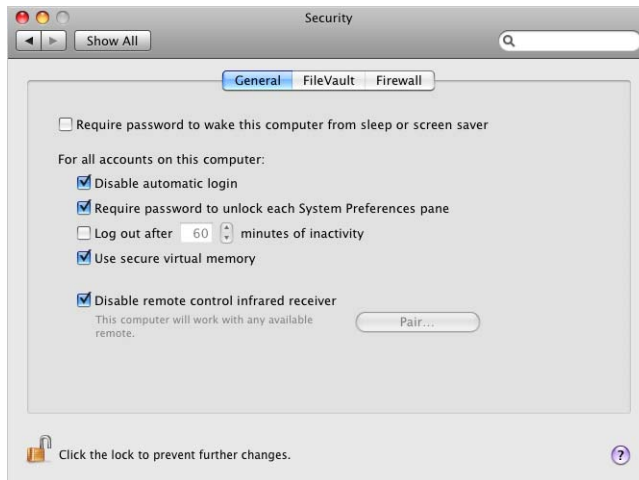


**To securely configure QuickTime preferences:**

- 1 Open QuickTime preferences.
- 2 In the Browser pane, deselect "Save movies in disk cache."

## Securing Security Preferences

The settings in Security preferences (shown here) cover a range of Mac OS X security features, including login options, FileVault, and firewall protection.



The settings under "For all accounts on this computer" require you to unlock Security preferences. Disable automatic login, require a password to unlock Security preferences, disable automatic logout because of inactivity, use secure virtual memory, and disable remote control infrared receivers.



## General Security

Consider the following general security guidelines:

- **Wake computer:** Require a password to wake this computer from sleep or screen saver. This helps prevent unauthorized access on unattended computers. Although there is a lock button for Security preferences, users don't need to be authorized as an administrator to make changes. Enable this password requirement for every user account on the computer.
- **Automatic login:** Disabling automatic login is necessary for any level of security. If you enable automatic login, an intruder can log in without authenticating. Even if you automatically log in with a restricted user account, it is still easier to perform malicious actions on the computer.
- **Password protect System Preferences:** Some system preferences are unlocked when you log in with an administrator account. By requiring a password, digital token, smart card, or biometric reader to unlock secure system preferences, you require extra authentication. This helps prevent accidental modification of system preferences.
- **Automatic logout:** Although you might want to enable automatic logout based on inactivity, there are reasons why you should disable this feature. First, it can disrupt your workflow. Second, it can close applications or processes without your approval (but a password-protected screen saver will not close applications). Third, because automatic logout can be interrupted, it provides a false sense of security. Applications can prevent successful automatic logout. For example, if you edit a file in a text editor, the editor might ask if you want to save the file before you log out.
- **Virtual memory:** Use secure virtual memory. The system's virtual memory swap file stores inactive physical memory contents, freeing your physical memory. By default on some systems, the swap file is unencrypted. This file can contain confidential data such as documents and passwords. By using secure virtual memory, you secure the swap file at a cost of slightly slower speed (because Mac OS X must encrypt and decrypt the secure swap file).
- **Infrared receiver:** If you are not using a remote control, disable the infrared receiver. This prevents unauthorized users from controlling your computer through the infrared receiver. If you use an Apple IR Remote Control, pair it to your computer by clicking Pair. When you pair it, no other IR remote can control your computer.

## FileVault Security

Mac OS X includes FileVault (see below), which encrypts information in your home folder.



FileVault uses the government-approved 128-bit (AES-128) encryption standard keys, and supports the Advanced Encryption Standard with 256-bit (AES-256) keys. For more information about data encryption, see Chapter 7, “Securing Data and Using Encryption.”

For more information about FileVault, see “Encrypting Home Folders” on page 139.

## Firewall Security

To enable a firewall that can block unauthorized programs from accepting new incoming network connections, use the Firewall pane (shown here). The firewall software also includes logging and stealth mode features.



**Note:** We recommend that you only allow essential services.

Advanced options include Enable Firewall Logging to provide information about firewall activity and Enable Stealth Mode to prevent the computer from sending responses to uninvited traffic.

### To securely configure Security preferences:

- 1 Open Security preferences.
- 2 Select the following:
  - “Require password to wake this computer from sleep or screen saver”
  - “Disable automatic login”
  - “Require password to unlock each System Preferences pane”
- 3 Deselect “Log out after # minutes of inactivity.”
- 4 Select the following:
  - “Use secure virtual memory”
  - “Disable remote control infrared receiver”
- 5 In the FileVault pane, select “Turn on FileVault.”
- 6 Authenticate with your account password.
- 7 Select “Use secure erase” and click “Turn on FileVault.”
- 8 In the Firewall pane, select one of the following:

- “Allow only essential services”
  - “Set access for specific services and applications”
- 9 If needed, click “Advanced” and select “Enable Firewall Logging” or “Enable Stealth Mode.”
  - 10 Add specific services and applications to the list.
  - 11 Restart the computer.

#### From the Command Line:

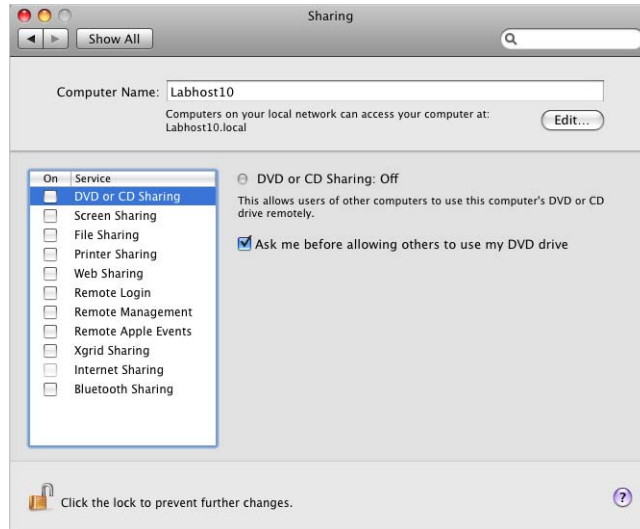
```
# Securing Security Preferences
# -----
# Enable Require password to wake this computer from sleep or screen saver.
defaults -currentHost write com.apple.screensaver askForPassword -int 1
# Disable Automatic login.
defaults write /Library/Preferences/.GlobalPreferences
com.apple.userspref.DisableAutoLogin -bool yes
# Requiring password to unlock each System Preference pane.
# Edit the /etc/authorization file using a text editor.
# Find <key>system.preferences<key>.
# Then find <key>shared<key>.
# Then replace <true/> with <false/>.
# Disable automatic login.
defaults write /Library/Preferences/.GlobalPreferences \
com.apple.autologout.AutoLogOutDelay -int 0
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
UseEncryptedSwap -bool yes
# Disable IR remote control.
defaults write /Library/Preferences/com.apple.driver.AppleIRController \
DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
/System/Library/CoreServices/ManagedClient.app/Contents/Resources/ \
createmobileaccount
# Enable Firewall.
# where value is
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
defaults write /Library/Preferences/com.apple.alf globalstate -int value
# Enable Stealth mode.
defaults write /Library/Preferences/com.apple.alf stealthenabled 1
# Enable Firewall Logging.
defaults write /Library/Preferences/com.apple.alf loggingenabled 1
```

## Securing Sharing Preferences

By default, every service listed in Sharing preferences is disabled. Do not enable these services unless you use them. The following services are described in detail in “Securing Network Sharing Services” on page 189.

Service	Description
DVD or CD Sharing	Allows users of other computers to remotely use the DVD or CD drive on your computer.
Screen Sharing	Allows users of other computers to remotely view and control the computer.
File Sharing	Gives users of other computers access to each user's Public folder.
Printer Sharing	Allows other computers to access a printer connected to this computer.
Web Sharing	Allows a network user to view websites located in /Sites. If you enable this service, securely configure the Apache web server.
Remote Login	Allows users to access the computer remotely by using SSH. If you require the ability to perform remote login, SSH is more secure than telnet, which is disabled by default.
Remote Management	Allows the computer to be accessed using Apple Remote Desktop.
Remote Apple Events	Allows the computer to receive Apple events from other computers.
Xgrid Sharing	Allows computers on a network to work together in a grid to process a job.
Internet Sharing	Allows other users to connect with computers on your local network, through your internet connection.
Bluetooth Sharing	Allows other Bluetooth-enabled computers and devices to share files with your computer.

You can change your computer's name in Sharing preferences, shown here.



By default your computer's host name is typically *firstname-lastname-computer*, where *firstname* and *lastname* are the system administrator's first name and last name, respectively, and *computer* is the type of computer or "Computer."

When users use Bonjour to discover available services, your computer appears as *hostname.local*. To increase privacy, change your computer's host name so you are not identified as the owner of your computer.

For more information about these services and the firewall and sharing capabilities of Mac OS X, see Chapter 12, "Information Assurance with Services."

#### To securely configure Sharing preferences:

- 1 Open Sharing preferences.
- 2 Change the default computer name to a name that does not identify you as the owner.

#### From the Command Line:

```
# Securing Sharing Preferences
# -----
# Change computer name where $host_name is the name of the computer.
systemsetup -setcomputername $host_name
# Change computer Bonjour host name.
# The host name cannot contain spaces or other non-DNS characters.
scutil --set LocalHostName $host_name
```

## Securing Software Update Preferences

Your Software Update preferences configuration depends on your organization's policy. For example, if your computer is connected to a managed network, the management settings determine what software update server to use.

Instead of using Software Update (shown here), you can also update your computer by using installer packages.



You can install and verify updates on a test computer before installing them on your operational computer. For more information about how to manually update your computer, see “Updating Manually from Installer Packages” on page 36.

After transferring installer packages to your computer, verify the authenticity of the installer packages. For more information, see “Repairing Disk Permissions” on page 37.

When you install a software update using Software Update or an installer package, you must authenticate with an administrator's name and password. This reduces the chance of accidental or malicious installation of software updates.

Software Update will not install a software package that has not been digitally signed by Apple.

### To disable automated Software Updates:

- 1 Open Software Update preferences.
- 2 Click the Scheduled Check pane.
- 3 Deselect “Download important updates automatically” and “Check for updates.”

### From the Command Line:

```
# Securing Software Updates Preferences
# -----
# Disable check for updates and Download important updates automatically.
softwareupdate --schedule off
```

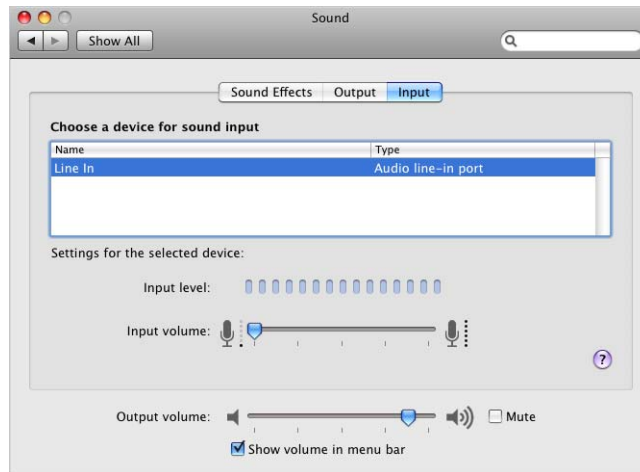
## Securing Sound Preferences

Many Apple computers include an internal microphone. You can use Sound preferences (shown below) to disable the internal microphone and the line-in port.

### To securely configure Sound preferences:

- 1 Open Sound preferences.

A screen similar to the following appears:



- 2 Select Internal microphone (if present), and set “Input volume” to zero.
- 3 Select Line-In (if present), and set “Input volume” to zero.

This ensures that “Line-In” is the device selected rather than the internal microphone when Sound preferences is closed. This provides protection from inadvertent use of the internal microphone.



## From the Command Line:

```
# Securing Sound Preferences
# -----
# Disable internal microphone or line-in.
# This command does not change the input volume for all input devices. It
# only sets the default input device volume to zero.
osascript -e "set volume input volume 0"
```

## Securing Speech Preferences

Mac OS X includes speech recognition and text-to-speech features, which are disabled by default.

Only enable these features if you work in a secure environment where no one can hear you speak to the computer or hear the computer speak to you. Also make sure no audio recording devices can record your communication with the computer.

The following shows the Speech Recognition preferences pane:



The following shows the Text to Speech pane:



If you enable text-to-speech, use headphones to keep others from overhearing your computer.

#### To customize Speech preferences:

- 1 Open Speech preferences.
- 2 Click the Speech Recognition pane and set Speakable Items On or Off.  
Change the setting according to your environment.
- 3 Click the Text to Speech pane and change the settings according to your environment.

#### From the Command Line:

```
# Securing Speech Preferences
# -----
# Disable Speech Recognition.
defaults write "com.apple.speech.recognition.AppleSpeechRecognition.prefs"
    StartSpeakableItems -bool false
# Disable Text to Speech settings.
defaults write "com.apple.speech.synthesis.general.prefs"
    TalkingAlertsSpeakTextFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
    SpokenNotificationAppActivationFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
    SpokenUIUseSpeakingHotKeyFlag -bool false
defaults delete "com.apple.speech.synthesis.general.prefs"
    TimeAnnouncementPrefs
```

## Securing Spotlight Preferences

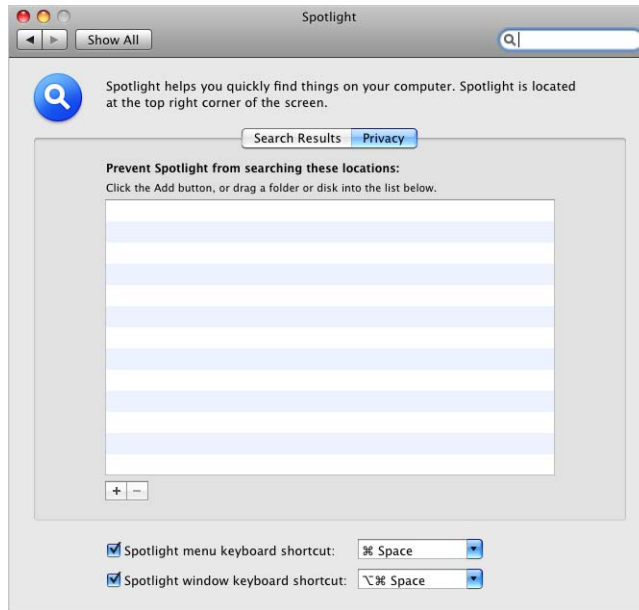
You can use Spotlight to search your computer for files. Spotlight searches the name, the meta-information associated with each file, and the contents of each file.

Spotlight finds files regardless of their placement in the file system. You must still properly set access permissions on folders containing confidential files. For more information about access permissions, see “Repairing Disk Permissions” on page 37.

The following is Spotlight Preferences Search Results pane.



By placing specific folders or disks in the Privacy pane (shown below), you can prevent Spotlight from searching them.



Disable the searching of folders that contain confidential information. Consider disabling top-level folders. For example, if you store confidential documents in subfolders of ~/Documents/, instead of disabling each folder, disable ~/Documents/.

By default, the entire system is available for searching using Spotlight.

#### To securely configure Spotlight preferences:

- 1 Open Spotlight preferences.
- 2 In the Search Results pane, deselect categories you don't want searchable by Spotlight.
- 3 Click the Privacy pane.
- 4 Click the Add button, or drag a folder or disk into the Privacy pane.

Folders and disks in the Privacy pane are not searchable by Spotlight.

#### From the Command Line:

```
# Securing Spotlight Preferences
# -----
# Disable Spotlight for a volume and erase its current meta data, where
# $volumename is the name of the volume.
$ mdutil -E -i off $volumename
```

For more information, enter `man mdutil` in a Terminal window.

## Securing Startup Disk Preferences

You can use Startup Disk preferences (shown below) to make your computer start up from a CD, a network volume, a different disk or disk partition, or another operating system.



Be careful when selecting a startup volume:

- Choosing a network install image reinstalls your operating system and might erase the contents of your hard disk.
- If you choose a FireWire volume, your computer starts up from the FireWire disk plugged into the current FireWire port for that volume. If you connect a different FireWire disk to that FireWire port, your computer starts from the first valid Mac OS X volume available to the computer (if you have not enabled the firmware password).
- When you enable a firmware password, the FireWire volume you select is the only volume that can start the computer. The computer firmware locks the FireWire Bridge Chip GUID as a startup volume instead of the hard disk's GUID (as is done with internal hard disks). If the disk inside the FireWire drive enclosure is replaced by a new disk, the computer can start from the new disk without using the firmware password. To avoid this intrusion make sure your hardware is physically secured. Your computer firmware can also have a list of FireWire volumes that are approved for system startup. For information about physically protecting your computer, see "Protecting Hardware" on page 41.

In addition to choosing a new startup volume from Startup Disk preferences, you can restart in Target Disk Mode. When your computer is in Target Disk Mode, another computer can connect to your computer and access your computer's hard disk. The other computer has full access to all files on your computer. All file permissions for your computer are disabled in Target Disk Mode.

To enter Target Disk Mode, hold down the T key during startup. You can prevent the startup shortcut for Target Disk Mode by enabling an Open Firmware or EFI password. If you enable an Open Firmware or EFI password, you can still restart in Target Disk Mode using Startup Disk preferences.

For more information about enabling an Open Firmware or EFI password, see “Using the Firmware Password Utility” on page 54.

**To select a startup disk:**

- 1 Open Startup Disk preferences.
- 2 Select a volume to use to start up your computer.
- 3 Click the “Restart” button to restart from the selected volume.

**From the Command Line:**

```
# Securing Startup Disk Preferences
# -----
# Set startup disk.
systemsetup -setstartupdisk $path
```

## Securing Time Machine Preferences

Time Machine (shown below) makes an up-to-date copy of everything on your Mac—digital photos, music, movies, downloaded TV shows, and documents—and lets you easily go “back in time” to recover files.

Time Machine is off by default. After you enable Time Machine for the first time no authentication is required and subsequent changes require authentication.

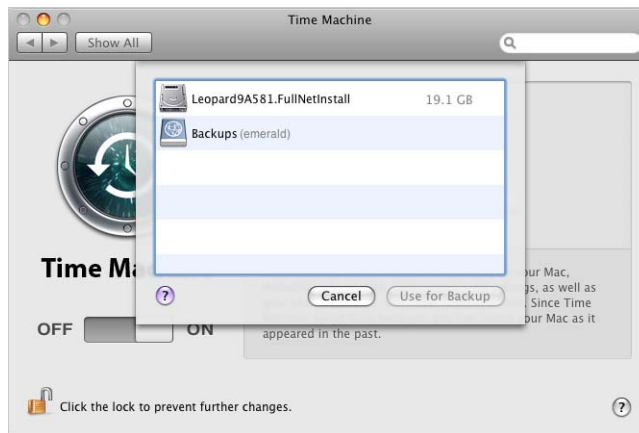
Information stored on your backup disk is not encrypted and can be read by other computers that are connected to your backup disk. Keep your backup disk in a physically secure location to prevent unauthorized access to your data.



**To enable Time Machine:**

- 1 Open Time Machine preferences.
- 2 Slide the switch to ON.

A screen similar to the following appears:



- 3 Select the disk where backups will be stored, and click Use for backup.

## From the Command Line:

```
# Securing Time Machine Preferences
# -----
# Enable Time Machine.
defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1
```

## Securing Universal Access Preferences

Universal Access preferences are disabled by default. If you don't use an assistive device there are no security-related issues. However, if you use an assistive device follow these guidelines:

- To prevent possible security risks, see the device manual.
- Enabling VoiceOver configures the computer to read the contents under the cursor out loud, which might disclose confidential data.
- These devices allow access to the computer that could reveal or store user input information.



Use this chapter to learn how to set POSIX, ACL, and global file permissions, to encrypt home folders and portable files, and to securely erase data.

Your data is the most valuable part of your computer. By using encryption you can protect data in case of an attack or theft of your mobile computer.

By setting global permissions, encrypting home folders, and encrypting portable data you can be sure your data is secure. In addition, by using the secure erase feature of Mac OS X, deleted data is completely erased from the computer.

## Understanding Permissions

You protect files and folders by setting permissions that restrict or allow users to access them. Mac OS X supports two methods of setting file and folder permissions:

- Portable Operating System Interface (POSIX) permissions—standard for UNIX operating systems.
- Access Control Lists (ACLs) permissions—used by Mac OS X, and compatible with Microsoft Windows Server 2003 and Microsoft Windows XP.

ACL uses POSIX when verifying file and folder permissions. The process ACL uses to determine if an action is allowed or denied includes verification rules called access control entries (ACEs). If no ACEs apply, standard POSIX permissions determine access.

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

## Setting POSIX Permissions

Mac OS X bases file permissions on POSIX standard permissions such as file ownership and access. Each share point, file, and folder has read, write, and execute permission defined for three categories of users: owner, group, and everyone. You can assign four types of standard POSIX access permissions to a share point, folder, or file: Read & Write, Read Only, Write Only, and None.

## Viewing POSIX Permissions

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

- Owner—A user who creates an item (file or folder) on the computer is its owner and has Read & Write permissions for that folder. By default the owner of an item and the administrator can change the item's access privileges (allow a group or everyone to use the item). The administrator can also transfer ownership of the shared item to another user.
- Group—You can put users who need the same access to files and folders into group accounts. Only one group can be assigned access permissions to a shared item. For more information about creating groups, see the *User Management* guide.
- Everyone—This is any user who can log in to the file server (registered users and guests).

Before setting or changing POSIX permissions, view the current permission settings.

### To view folder or file permissions:

- 1 Open Terminal.
- 2 Run the `ls` command:

```
$ ls -l
```

Output similar to the following appears:

```
computer:~/Documents ajohnson$ ls -l
total 500
drwxr-xr-x  2 ajohnson staff   68 Apr 28 2006 NewFolder
-rw-r--r--  1 ajohnson staff 43008 Apr 14 2006 file.txt
```

**Note:** The “~” refers to your home folder, which in this case is `/Users/ajohnson`.  
`~/Documents/` is the current working folder.

You can also use the Finder to view POSIX permissions. In the Finder, Control-click a file and choose Get Info. Open the Ownership & Permissions disclosure triangle to view POSIX permissions.

## Interpreting POSIX Permissions

To interpret POSIX permissions, read the first 10 bits of the long format output listed for a file or folder.

```
drwxr-xr-x 2 ajohnson staff    68 Apr 28 2006 NewFolder
-rw-r--r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

In this example, `NewFolder` has the POSIX permissions `drwxr-xr-x` and has an owner and group of `ajohnson`. Permissions are as follows:

- The `d` of the POSIX permissions signifies that `newfolder` is a folder.
- The first three letters after the `d` (`rxw`) signify that the owner has read, write, and execute permissions for that folder.
- The next three characters, `r-x`, signify that the group has read and execute permissions.
- The last three characters, `r-x`, signify that all others have read and execute permissions.

In this example, users who can access `ajohnson's ~/Documents/` folder can open the `NewFolder` folder but can't modify or open the `file.txt` file. Read POSIX permissions are propagated through the folder hierarchy.

Although `NewFolder` has `drwxr-xr-x` privileges, only `ajohnson` can access the folder. This is because `ajohnson's ~/Documents/` folder has `drwx-----` POSIX permissions.

By default, most user folders have `drwx-----` POSIX permissions. Only the `~/`, `~/Sites/`, and `~/Public/` folders have `drwxr-xr-x` permissions. These permissions allow other people to view folder contents without authenticating. If you don't want other people to view the contents, change the permissions to `drwx-----`.

In the `~/Public/` folder, the Drop Box folder has `drwx-wx-wx` POSIX permissions. This allows other users to add files into `ajohnson's drop box` but they can't view the files.

You might see a `t` for others' privileges on a folder used for collaboration. This `t` is sometimes known as the sticky bit. Enabling the sticky bit on a folder prevents people from overwriting, renaming, or otherwise modifying other people's files. This can be common if several people are granted `rxw` access.

The sticky bit can appear as `t` or `T`, depending on whether the execute bit is set for others:

- If the execute bit appears as `t`, the sticky bit is set and has searchable and executable permissions.
- If the execute bit appears as `T`, the sticky bit is set but does not have searchable or executable permissions.

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

## Modifying POSIX Permissions

After you determine current POSIX permission settings, you can modify them using the `chmod` command.

**To modify POSIX permission:**

- 1 In Terminal, enter the following to add write permission for the group to `file.txt`:

```
$ chmod g+w file.txt
```

- 2 View the permissions using the `ls` command.

```
$ ls -l
```

- 3 Validate that the permissions are correct.

```
computer:~/Documents ajohnson$ ls -l
total 12346
drwxr-xr-x 2 ajohnson staff   68 Apr 28 2006 NewFolder
-rw-rw-r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

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

## Setting File and Folder Flags

You can also protect files and folders by using flags. These flags, or permission extensions, override standard POSIX permissions. They can only be set or unset by the file's owner or an administrator using `sudo`. Use flags to prevent the system administrator (root) from modifying or deleting files or folders.

To enable and disable flags, use the `chflags` command.

### Viewing Flags

Before setting or changing file or folder flags, view the current flag settings.

**To display flags set on a folder:**

```
$ ls -lo secret
-rw-r--r-- 1 ajohnson ajohnson uchg 0 Mar  1 07:54 secret
```

This example displays the flag settings for a folder named `secret`.

### Modifying Flags

After you determine current file or folder flag settings, modify them using the `chflags` command.

**To lock or unlock a folder using flags:**

```
$ sudo chflags uchg secret
```

In this example, the folder named `secret` is locked.

To unlock the folder, change `uchg` to `nouchg`:

```
$ sudo chflags nouchg secret
```

**WARNING:** There is an `schg` option for the `chflags` command. It sets the system immutable flag. This setting can only be undone when the computer is in single-user mode. If this is done on a RAID, XSan, or other storage device that cannot be mounted in single user mode, the only way to undo the setting is to reformat the RAID or XSan device.

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

## Setting ACL Permissions

For greater flexibility in configuring and managing file permissions, Mac OS X implements ACLs. An ACL is an ordered list of rules called ACEs that control file permissions. Each ACE contains the following components:

- User—owner, group, and other
- Action—read, write, or execute
- Permission—allow or deny the action

The rules specify the permissions to be granted or denied to a group or user and controls how the permissions are propagated through a folder hierarchy.

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

Mac OS X has implemented file system ACLs that are fully compatible with Microsoft Windows Server 2003, Windows Server 2008, Windows XP, and Windows Vista.

To determine if an action is allowed or denied, ACEs are considered in order. The first ACE that applies to a user and action determines the permission and no further ACEs are evaluated. If no ACEs apply, standard POSIX permissions determine access.

## Modifying ACL Permissions

You can set ACL permission for files. The `chmod` command enables an administrator to grant read, write, and execute privileges to specific users regarding a single file.

### To set ACL permissions for a file:

- 1 Allow specific users to access specific files.

For example, to allow Anne Johnson permission to read the file `secret.txt`, enter the following in Terminal:

```
$ chmod +a "ajohnson allow read" secret.txt
```

## 2 Allow specific groups of users to access specific files.

For example, to allow the engineers group permission to delete the file secret.txt, enter the following in Terminal:

```
$ chmod +a "engineers allow delete" secret.txt
```

## 3 Deny access privileges to specific files.

For example, to prevent Tom Clark from modifying the file secret.txt, enter the following in Terminal:

```
$ chmod +a "tclark deny write" secret.txt
```

## 4 View and validate the ACL modifications with the `ls` command:

```
$ ls -le secret.txt
-rw----- 1 ajohnson admin 43008 Apr 14 2006 secret.txt
0: ajohnson allow read
1: tclark deny write
2: engineers allow delete
```

For more information, enter `man chmod` in a Terminal window.

## Changing Global Umask for Stricter Default Permissions

Every file or folder has POSIX permissions associated with it. When you create a file or folder, the umask setting determines these POSIX permissions.

The umask value is subtracted from the maximum permissions value (777) to determine the default permission value of a newly created file or folder. For example, a umask of 022 results in a default permission of 755.

The default umask setting 022 (in octal) removes group and other write permissions. Group members and other users can read and run these files or folders. Changing the umask setting to 027 enables group members to read files and folders and prevents others from accessing the files and folders. If you want to be the only user to access your files and folders, set the umask setting to 077.

To change the globally defined umask setting, change the umask setting in `/etc/launchd.conf`.

You must be logged in as a user who can use `sudo` to perform these operations and you must use the decimal equivalent, not an octal number.

**Note:** Users and applications can override default umask settings at any time for their own files.

**WARNING:** Many installations depend on the default umask setting. There can be unintended and possibly severe consequences to changing it. Instead, use inherited permissions, which are applied by setting permissions on a folder. All files contained in that folder will inherit the permissions of that folder.

**To change the global umask file permission:**

- 1 Sign in as a user who can use `sudo`.
- 2 Open Terminal.
- 3 Change the umask setting:  

```
$ sudo echo "umask 027" >> /etc/launchd.conf
```

This example sets the global umask setting to 027.
- 4 Log out.

Changes to umask settings take effect at the next login.

Users can use the Finder's Get Info window or the `chmod` command-line tool to change permissions for files and folders.

## Restricting Setuid Programs

When applied to a program, the POSIX setuid (set user ID) permission means that when the program runs, it will run at the privilege level of the file's owner. The POSIX setgid (set group ID) permission is analogous. To see an example of a file with the setuid bit, run the `ls` command on the `ping` program as follows:

```
$ ls -l /sbin/ping
-r-sr-xr-x 1 root  wheel  68448 Nov 28  2007 /sbin/ping
```

The setuid bit is represented with an 's' in the field of permissions, in the position that contains the file owner's execute permission. The program runs with the privilege level of the file's owner. The owner of the file is `root`, so when `ping` is executed—no matter who actually executes it—it runs as `root`. For setgid programs, an 's' appears in the group execute permission and the file runs with the privileges of the group owner.

The setuid bit is necessary in order for many programs on the system to perform the specific, privileged tasks for which they are designed. The `ping` program, for example, is setuid because it needs to be able to engage in some network communication that is only possible with root privileges.

**To find setuid programs on the system, use the following command:**

```
$ sudo find / -perm -04000 -ls
```

To find setgid programs, use -02000 instead of -04000.

Mac OS X includes approximately 75 setuid programs. Many of these programs need the setuid bit for normal system operation. However, other programs may need the setuid bit only if certain functionality is needed, or only if administrators need to use the program. Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program. If a program is needed but has had its setuid bit stripped, an administrator can run the program using `sudo`, which runs the program as the root user. An administrator can also temporarily enable the setuid bit while the program is needed, and then disable it again afterward.

### Stripping Setuid Bits

**To strip the setuid or setgid bit from a program, use the following command:**

```
$ sudo chmod -s programname
```

The following programs can have their setuid bit removed, unless needed for the purpose shown in the second column:

Application	Related Service
/System/Library/CoreServices/ RemoteManagement/ ARDAgent.app/Contents/ MacOS/ARDAgent	Apple Remote Desktop
/System/Library/Extensions/ webdav_fs.kext/Contents/ Resources/load_webdav	WebDAV Web Services
/System/Library/Filesystems/ AppleShare /afpLoad	Apple File Protocol
/System/Library/Filesystems/ AppleShare/check_afp.app/ Contents/MacOS/check_afp	Apple File Protocol Sharing
/System/Library/Frameworks/ ApplicationServices.framework/ Versions/A/Frameworks/ PrintCore.framework/Versions/A/ Resources/PrinterSharingTool	Printer Sharing
/System/Library/CoreServices/ Expansion Slot Utility.app/ Contents/ Resources/PCIELaneConfigTool	Expansion Slot Utility



Application	Related Service
/System/Library/PrivateFrameworks/DesktopServicesPriv.framework/Versions/A/Resources/Locum	Performing Privileged File Operations using Finder
/System/Library/Printers/Libraries/aehelper	Printer Configuration
/System/Library/Printers/Libraries/csmregprinter	Printer Configuration
/System/Library/PrivateFrameworks/DiskManagement.framework/Versions/A/Resources/DiskManagementTool	Disk Utility
/usr/libexec/dumpemacs	N/A
/usr/libexec/xgrid/IdleTool	XGrid
/usr/libexec/statsCollector	Network BigTop
/usr/sbin/vpnd	Hosting VPN Services
/sbin/mount_nfs	Mounting NFS Filesystems
/sbin/route	Network Configuration
/usr/bin/lppasswd	Printer Sharing
/usr/bin/ipcs	IPC Statistics
/bin/rcp	Remote Access (unsecure)
/usr/bin/rlogin	Remote Access (unsecure)
/usr/bin/rsh	Remote Access (unsecure)
/usr/lib/sa/sadc	System Activity Reporting
/usr/sbin/pppd	PPP
/usr/sbin/scselect	Allowing non-administrators to change Network Location

**Important:** The "Repair Permissions" feature of Disk Utility re-enables the setuid bit on these programs. Software updates may also re-enable the setuid bit on these programs. In order to achieve some persistence for the permissions change, create a shell script to strip the bits and then implement a cron job (for the root account) to execute this script every half hour. This ensures that no more than half an hour passes from the time a system update is applied until the setuid bits are removed. For information about how to set up a cron job, consult *Command-Line Administration*, available at <http://www.apple.com/server/macosx/resources/>.

## Using ACLs to Restrict Usage of Setuid Programs

The ACL feature of Mac OS X can also be used to restrict the execution of setuid programs. Restricting the execution of setuid programs to administrators prevents other users from executing those programs. It should also prevent attackers who are currently running with ordinary user privileges from executing the setuid program and trying to elevate their privileges. All users on the system are in the “staff” group, so the commands below allow members of the admin group to execute <program name>, but deny that right to members of the staff group:

```
$ sudo chmod +a "group:staff deny execute" <program name>
$ sudo chmod +a# 0 "group:admin allow execute" <program name>
```

### To view the ACL:

```
$ ls -le <program name>
```

The output looks something like this:

```
-r-sr-xr-x+ 1 root wheel 12345 Nov 28 2007 <program name>
0: group:admin allow execute
1: group:staff deny execute
```

Because the ACL is evaluated in order from top to bottom, users in the admin group are permitted to execute the program. The following rule denies that right to all users.

**Important:** Although the “Repair Permissions” feature of Disk Utility does not strip ACLs from programs, software updates might strip these ACLs. In order to achieve some persistence for the ACLs, create a shell script to set the ACLs and then implement a cron job (for the root account) to execute this script. For information about how to set up a cron job, consult *Command-Line Administration*, available at <http://www.apple.com/server/macosx/resources/>.

A cron job should ensure that no longer than an understood time period should pass from the time a system update is applied and the ACL is reset. Because the ACL described above uses the +a# option to place rules in a non-canonical order, its reapplication results in additional rules. The following script can successfully apply – and reapply – the rules:

```
chmod -a "group:admin allow execute" <program name>
chmod +a "group:staff deny execute" <program name>
chmod +a# 0 "group:admin allow execute" <program name>
```

## Securing User Home Folders

To secure user home folders, change the permissions of each user’s home folder so the folder is not world-readable or world-searchable.

When FileVault is not enabled, the permissions on the home folder of a new user account allow other users to browse the folder's contents. However, users might inadvertently save sensitive files to their home folder, instead of into the more-protected ~/Documents, ~/Library, or ~/Desktop folders.

The ~/Sites, ~/Public, and ~/Public/Drop Box folders in each home folder may require world-readable or world-writeable permissions if File Sharing or Web Sharing is enabled. If these services are not in use, the permissions on these folders can be safely changed to prevent other users from browsing or writing to their contents.

### To change home folder permissions:

Enter the following command:

```
$ sudo chmod 700 /Users/username
```

Replace *username* with the name of the account.

Run this command immediately after someone creates an account.

In Mac OS X version 10.5 Leopard all users are a member of the "staff" group, not of a group that has the same name as their user name.

**Note:** Changing permissions on a user's home directory from 750 to 700 will disable Apple file sharing (using the ~/Public directory) and Apple web sharing (using the ~/Sites directory).

As the owner of his or her home folder, the user can alter the folder's permission settings at any time, and can change these settings back.

## Encrypting Home Folders

Mac OS X includes FileVault, which can encrypt your home folder and its files. Use FileVault on portable computers and other computers whose physical security you can't guarantee. Enable FileVault encryption for your computer and its user accounts.

FileVault moves all content of your home folder into a bundle disk image that supports AES-256 encryption. Mac OS X Leopard supports the Mac OS X version 10.4 Tiger sparse disk image format created using AES-128 encryption. The sparse format allows the image to maintain a size proportional to its contents, which can save disk space.

If you remove files from a FileVault-protected home folder it takes time to recover free space from the home folder. After the home folder is optimized, you can access files in FileVault-protected home folders without noticeable delays.

If you're working with confidential files that you plan to erase later, store those files in separate encrypted images that are not located in your home folder. You can then erase those images without needing to recover free space. For more information, see "Encrypting Portable Files" on page 143.

If you've insecurely deleted files before using FileVault, these files are recoverable after activating it. When you initially enable FileVault, securely erase free space. For information, see "Using Disk Utility to Securely Erase Free Space" on page 148.

Because FileVault is an encryption of a user's local home folder, FileVault does not encrypt or protect files transferred over the network or saved to removable media, so you'll need to encrypt specific files or folders. FileVault can only be enabled for local or mobile accounts and cannot be enabled for network home folders.

If you want to protect file or folders on portable media or a network volume, you must create an encrypted disk image on the portable media or network volume. You can then mount these encrypted disk images, which protect data transmitted over the network using AES-256 encryption. When using this method, you must only mount the encrypted disk image from one computer at a time to prevent irreparable corruption to the image content.

For information about encrypting specific files or folders for transfer from your network home folder, see "Encrypting Portable Files" on page 143.

When you set up FileVault, you create a master password. If you forget your login password, you can use your master password to recover encrypted data. If you forget your login password and your master password, you cannot recover your data. Because of this, consider sealing your master password in an envelope and storing it in a secure location.

You can use Password Assistant to help create a complex master password that cannot be easily compromised. For information, see "Using Password Assistant to Generate or Analyze Passwords" on page 73.

Enabling FileVault copies data from your home folder into an encrypted home folder. After copying, FileVault erases the unencrypted data.

By default FileVault insecurely erases the unencrypted data, but if you enable secure erase, your unencrypted data is securely erased.

## Overview of FileVault

Mac OS X Leopard allows the unlocking of FileVault accounts by Smart Cards, which provides the most secure practice for protecting FileVault accounts.

Accounts protected by FileVault support authentication using a passphrase or a Smart Card. With Smart Card authentication, the AES-256 symmetric Data Key (DK) used to encrypt the user's data is unwrapped using a private (encryption) key on the Smart Card. The data written to or read from disk is encrypted and decrypted on the fly during access.

FileVault encrypts the Data Key (DK) using the User Key (UK1), which can be generated from your passphrase or from the public key on your Smart Card. FileVault separately encrypts the Data Key using the FileVault Master Key (MK).

The architectural design of FileVault makes it possible for the MK and UK1 to encrypt and decrypt files. Providing strong encryption protects user data at rest while ensuring access management by IT staff.

The easiest method for centralized management of FileVault on a client computer is to use Mac OS X version 10.5 Leopard Server and WorkGroup Manager to enforce the use of FileVault and the proper identity.

## Managing FileVault

You can set a FileVault master keychain to decrypt an account that uses FileVault to encrypt data. Then if users forget their FileVault account password (which they use to decrypt encrypted data), you can use the FileVault master keychain to decrypt the data.

### To create the FileVault master keychain:

- 1 Open System Preferences.
- 2 Click Security, then click FileVault.
- 3 Click Master Password and set a master password.

Select a strong password and consider splitting the password into at least two components (first half and second half). You can use Password Assistant to ensure that the quality of the password is strong.

To avoid having one person know the full password, have separate security administrators keep each password component. This prevents a single person from unlocking (decrypting) a FileVault account. For more information about Password Assistant, see "Using Password Assistant to Generate or Analyze Passwords" on page 73.

This creates a keychain called FileVaultMaster.keychain in /Library/Keychains/. The FileVault master keychain contains a FileVault recovery key (self-signed root certificate) and a FileVault master password key (private key).

- 4 Delete the certificate named FileVaultMaster.cer in the same location as the FileVaultMaster.keychain.

FileVaultMaster.cer is only used for importing the certificate into the keychain. This is only a certificate and does not contain the private key, so there is no security concern about someone gaining access to this certificate.

- 5 Make a copy of FileVaultMaster.keychain and put it in a secure place.
- 6 Delete the private key from FileVaultMaster.keychain created on the computer to modify the keychain.

This ensures that even if someone unlocks the FileVault master keychain they cannot decrypt the contents of a FileVault account because there is no FileVault master password private key available for decryption.

### Managing the FileVault Master Keychain

The modified FileVault master keychain can now be distributed to network computers. This can be done by transferring FileVaultMaster.keychain to the computers by using Apple Remote Desktop, by using a distributed installer executed on each computer, by using various scripting techniques, or by including it in the original disk image if your organization restores systems with a default image.

This provides network management of any FileVault account created on any computer with the modified FileVaultMaster.keychain located in the /Library/Keychains/ folder. These computers indicate that the master password is set in Security preferences.

When an account is created and the modified FileVault master keychain is present, the public key from the FileVault recovery key is used to encrypt the dynamically generated AES 256-bit symmetric key used for encryption and decryption of the encrypted disk image (FileVault container).

To decrypt access to the encrypted disk image, the FileVault master password private key is required to decrypt the original dynamically generated AES 128-bit or 256-bit symmetric key. The user's original password continues to work as normal, but the assumption here is that the master password service is being used because the user has forgotten the password or the organization must perform data recovery from a user's computer.

#### To recover a network-managed FileVault system account:

- 1 Retrieve the copy of FileVaultMaster.keychain that was stored before the private key was deleting during modification.
- 2 If the master password was split into password components, bring together all security administrators involved in generating the master password.

**Note:** The administrator must have root access to restore FileVaultMaster.keychain.

- 3 Restore the original keychain to the /Library/Keychains/ folder of the target computer replacing the installed one.
- 4 Verify that the restored FileVaultMaster.keychain file has the correct ownership and permissions set, similar to the following example.

```
-rw-r--r-- 1 root admin 24880 Mar 2 18:18 FileVaultMaster.keychain
```

- 5 Log in to the FileVault account you are attempting to recover and incorrectly enter the account password three times.

If “Password Hints” is enabled, you are granted an additional try after the hint appears.

- 6 When prompted for the master password, have the security administrators combine their password components to unlock access to the account.

- 7 When the account is unlocked, provide a new password for the account.

The password is used to encrypt the original symmetric key used to encrypt and decrypt the disk image.

**Note:** This process does not reencrypt the FileVault container. It reencrypts the original symmetric key with a key derived from the new user account password you entered.

You are now logged in to the account and given access to the user’s home folder.

- 8 Delete the private key from FileVaultMaster.keychain again, or replace the keychain file with the original copy of FileVaultMaster.keychain that was stored before the private key was deleted.

This process does not change the password used to protect the user’s original login keychain, because that password is not known or stored anywhere. Instead, this process creates a login keychain with the password entered as the user’s new account password.

## Encrypting Portable Files

To protect files you want to transfer over a network or save to removable media, encrypt a disk image or encrypt the files and folders. FileVault doesn’t protect files transmitted over the network or saved to removable media.

Using a server-based encrypted disk image provides the added benefit of encrypting network traffic between the computer and the server hosting the mounted encrypted disk image.

## Creating an Encrypted Disk Image

To encrypt and securely store data, you can create a read/write image or a sparse image:

- A read/write image consumes the space that was defined when the image was created. For example, if the maximum size of a read/write image is set to 10 GB, the image consumes 10 GB of space even if it contains only 2 GB of data.
- A sparse image consumes only the amount of space the data needs. For example, if the maximum size of a sparse image is 10 GB and the data is only 2 GB, the image consumes only 2 GB of space.

If an unauthorized administrator might access your computer, creating an encrypted blank disk image is preferred to creating an encrypted disk image from existing data.

Creating an encrypted image from existing data copies the data from an unprotected area to the encrypted image. If the data is sensitive, create the image before creating the documents. This creates the working copies, backups, or caches of files in encrypted storage from the start.

**Note:** To prevent errors when a file system inside a sparse image has more free space than the volume holding the sparse image, HFS volumes inside sparse images report an amount of free space slightly less than the amount of free space on the volume the image resides on.

**To create an encrypted disk image:**

- 1 Open Disk Utility.
- 2 Choose File > New > Blank Disk Image.
- 3 Enter a name for the image, and choose where to store it.
- 4 Choose the size of the image, by clicking the Size pop-up menu.  
Make sure the size of the image is large enough for your needs. You cannot increase the size of an image after creating it.
- 5 Choose an encryption method by clicking the Encryption pop-up menu.  
AES-128 or AES-256 is a strong encryption format.
- 6 Choose a format by clicking the Format pop-up menu.  
Although there is some overhead, the sparse format allows the image to maintain a size proportional to its contents (up to its maximum size), which can save disk space.
- 7 Click Create.
- 8 Enter a password and verify it.  
You can access Password Assistant from this window. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.
- 9 Deselect “Remember password (add to Keychain)” and click OK.

### Creating an Encrypted Disk Image from Existing Data

If you must maintain data confidentiality when transferring files from your computer but you don’t need to encrypt files on your computer, create a disk image from existing data.

Such situations include unavoidable plain text file transfers across a network, such as mail attachments or FTP, or copying to removable media, such as a CD or floppy disk.

If you plan to add files to this image instead of creating an image from existing data, create an encrypted disk image and add your existing data to it. For information, see “Creating an Encrypted Disk Image” on page 143.



**To create an encrypted disk image from existing data:**

- 1 Open Disk Utility.
- 2 Choose File > New > Disk Image from Folder.
- 3 Select a folder, and click Image.
- 4 Choose File > New > Blank Disk Image.
- 5 Enter a name for the image and choose where to store it.
- 6 Choose a format by clicking the Format pop-up menu.

The compressed disk image format can help you save hard disk space by reducing your disk image size.
- 7 Choose an encryption method by clicking the Encryption pop-up menu.

AES-128 or AES-256 provide strong encryption.
- 8 Click Save.
- 9 Enter a password and verify it.

You can easily access Password Assistant from this window. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.
- 10 Deselect “Remember password (add to Keychain)” and click OK.

## Creating Encrypted PDFs

You can quickly create password protected, read-only PDF documents of confidential or personal data. To open these files you must know the password for them.

Some applications do not support printing to PDF. In this case, create an encrypted disc image. For information, see “Creating an Encrypted Disk Image from Existing Data” on page 144.

**To create an encrypted PDF, read-only document:**

- 1 Open the document.
- 2 Choose File > Print.

Some applications don’t allow you to print from the File menu. These applications might allow you to print from other menus.
- 3 Click PDF and choose Save as PDF.
- 4 Click Security Options and select one or more of the following options:
  - Require password to open document
  - Require password to copy text images and other content
  - Require password to print document

When you require a password for the PDF, it becomes encrypted.
- 5 Enter a password, verify it, and click OK.

- 6 Enter a name for the document, choose a location, and click Save.
- 7 Test your document by opening it.

You must enter the password before you can view the contents of your document.

## Securely Erasing Data

When you erase a file, you're removing information that the file system uses to find the file. The file's location on the disk is marked as free space. If other files have not written over the free space, it is possible to retrieve the file and its contents.

Mac OS X provides the following ways to securely erase files.

- Zero-out erase
- 7-pass erase
- 35-pass erase

A zero-out erase sets all data bits on the disk to 0, while a 7-pass erase and a 35-pass erase use algorithms to overwrite the disk. A 7-pass erase follows the Department of Defense standard for the sanitization of magnetic media. A 35-pass erase uses the extremely advanced Gutmann algorithm to help eliminate the possibility of data recovery.

The zero-out erase is the quickest. The 35-pass erase is the most secure, but it is also 35 times slower than the zero-out erase.

Each time you use a 7-pass or 35-pass secure erase, the following seven-step algorithm is used to prevent the data from ever being recovered:

- Overwrite file with a single character
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters

## Configuring Finder to Always Securely Erase

In Mac OS X Leopard you can configure Finder to always securely erase items placed in the Trash. This prevents data you place in the Trash from being restored. Using secure erase take longer than emptying the Trash.

To configure Finder to always perform a secure erase:

- 1 In Finder, choose Finder > Preferences.
- 2 Click Advanced.

- 3 Select the “Empty Trash securely” checkbox.

## Using Disk Utility to Securely Erase a Disk or Partition

You can use Disk Utility to securely erase a partition, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

**Note:** If you have a partition with Mac OS X installed and you want to securely erase an unmounted partition, you don’t need to use your installation discs. In the Finder, open Disk Utility (located in /Applications/Utilities/).

**WARNING:** Securely erasing a partition is irreversible. Before erasing the partition, back up critical files you want to keep.

### To securely erase a partition using Disk Utility:

- 1 Insert the first of the Mac OS X installation discs in the optical drive.
- 2 Restart the computer while holding down the C key.  
The computer starts up from the disc in the optical drive.
- 3 Proceed past the language selection step.
- 4 Choose Utilities > Disk Utility.
- 5 Select the partition you want to securely erase.  
Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.
- 6 Click Erase, choose “Mac OS Extended Journaled,” and then click Security Options.  
Mac OS Extended disk formatting provides enhanced multiplatform interoperability.
- 7 Choose an erase option and click OK.
- 8 Click Erase.  
Securely erasing a partition can take time, depending on the size of the partition and the method you choose.

## Using Command-Line Tools to Securely Erase Files

You can use the `srm` command in Terminal to securely erase files or folders. By using `srm`, you can remove each file or folder by overwriting, renaming, and truncating the file or folder before erasing it. This prevents other people from undeleting or recovering information about the file or folder.

For example, `srm` supports simple methods, like overwriting data with a single pass of zeros, to more complex ones, like using a 7-pass or 35-pass erase.

The `srm` command cannot remove a write-protected file owned by another user, regardless of the permissions of the directory containing the file.

**WARNING:** Erasing files with `srm` is irreversible. Before securely erasing files, back up critical files you want to keep.

**To securely erase a folder named `secret`:**

```
$ srm -r -s secret
```

The `-r` option removes the content of the directory and the `-s` option (simple) overwrites with a single random pass.

For a more secure erase, use the `-m` (medium) option to perform a 7-pass erase of the file. The `-s` option overrides the `-m` option if both are present. If neither is specified, the 35-pass is used.

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

## Using Secure Empty Trash

Secure Empty Trash uses a 7-pass erase to securely erase files stored in the Trash.

Depending on the size of the files being erased, securely emptying the Trash can take time to complete.

**WARNING:** Using Secure Empty Trash is irreversible. Before securely erasing files, back up critical files you want to keep.

**To use Secure Empty Trash:**

- 1 Open the Finder.
- 2 Choose Finder > Secure Empty Trash.
- 3 Click OK.

## Using Disk Utility to Securely Erase Free Space

You can use Disk Utility to securely erase free space on partitions, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

**To securely erase free space using Disk Utility:**

- 1 Open Disk Utility (located in `/Applications/Utilities/`).
- 2 Select the partition to securely erase free space from.

Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.

- 3 Click Erase and then click Erase Free Space.
- 4 Choose an erase option and click Erase Free Space.

Securely erasing free space can take time, depending on the amount of free space being erased and the method you choose.

- 5 Choose Disk Utility > Quit Disk Utility.

## Using Command-Line Tools to Securely Erase Free Space

You can securely erase free space from the command line by using the `diskutil` command. However, ownership of the affected disk is required. This tool allows you to securely erase using one of the three levels of secure erase:

- 1—Zero-out secure erase (also known as single-pass)
- 2—7-pass secure erase
- 3—35-pass secure erase

**To erase free space using a 7-pass secure erase (indicated by the number 2):**

```
$ diskutil secureErase freespace 2 /dev/disk0s3
```

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



Use this chapter to protect data in swap files from being readable.

The data that an application writes to random-access memory (RAM) might contain sensitive information, such as user names and passwords. Mac OS X writes the contents of RAM to your local hard disk to free memory for other applications. The RAM contents stored on the hard disk are kept in a file called a swap file.

While the data is on the hard disk, it can be easily viewed or accessed if the computer is later compromised. You can protect this data by securing the system swap file in case of an attack or theft of your computer.

## System Swap File Overview

When your computer is turned off, any information stored in RAM is lost, but information stored by virtual memory in a swap file may remain on your hard drive in unencrypted form. The Mac OS X virtual memory system creates this swap file in order to reduce problems caused by limited memory.

The virtual memory system can swap data between your hard disk and RAM. It's possible that sensitive information in your computer's RAM will be written to your hard disk in the swap file while you are working, and remain there until overwritten. This data can be compromised if your computer is accessed by an unauthorized user, because the data is stored on the hard disk unencrypted.

When your computer goes into hibernation, it writes the content of RAM to the `/var/vm/sleepimage` file. The sleepimage file contains the contents of RAM unencrypted, similar to a swap file.

You can prevent your sensitive RAM information from being left unencrypted on your hard disk by enabling secure virtual memory to encrypt the swap file and the `/var/vm/sleepimage` file (where your hibernation files are stored).

**Note:** Using FileVault in combination with the “Secure Virtual Memory” feature provides protection from attacks on your sensitive data when it is stored on the hard drive.

## Encrypting System Swap

You can prevent your sensitive information from remaining on your hard disk and eliminate the security risk by using secure virtual memory. Secure virtual memory encrypts the data being written to disk.

### To turn on secure virtual memory:

- 1 Open System Preferences.
- 2 Click Security, then click General.
- 3 Select “Use secure virtual memory.”
- 4 Reboot.

### From the Command Line:

```
# Securing System Swap and Hibernation Storage
# -----
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
    UseEncryptedSwap -bool YES
```



Use this chapter to limit local account access so you can more easily monitor activity on your computer.

Monitoring user accounts and activities is important to securing your computer. This enables you to determine if an account is compromised or if a user is performing malicious tasks.

## Fast User Switching

Although the use of Fast User Switching is convenient when you have multiple users on a single computer, there are cases in which you may not want to enable it.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is using the computer.

Also, some external volumes attached to the computer are mounted when another user logs in, granting all users access to the volume and ignoring access permissions.

## Shared User Accounts

Avoid creating accounts that are shared by several users. Individual accounts maintain accountability. Each user should have his or her own standard or managed account.

System logs can track activities to each user account, but if several users share the same account, it becomes difficult to track which user performed an activity. Similarly, if several administrators share a single administrator account, it becomes harder to track which administrator performed a specific action.

If someone compromises a shared account it is less likely to be noticed. Users might mistake malicious actions performed by an intruder for legitimate actions by a user sharing the account.



Use this chapter to learn about secure ways of backing up data and preventing unauthorized access to backups.

Most organizations perform backups to protect data from being lost. However, many organizations don't consider that their backups can be compromised if not securely stored on media.

## Understanding the Time Machine Architecture

Time Machine is based on the Mac OS X HFS+ file system. It tracks file changes and detects file system permissions and user access privileges.

When Time Machine performs the initial backup, it copies the contents of your computer to your backup disk. Every subsequent backup is an incremental backup, which copies only the files that have changed since the previous backup.

## Deleting Permanently from Time Machine backups

You can permanently delete files or folders from your computer and Time Machine backups using Time Machine. This prevents any old sensitive data that you no longer need from being recovered.

### To permanently delete files or folders from Time Machine backups:

- 1 Delete the file or folder from your computer.
  - 2 Open Time Machine.
  - 3 Select the file or folder you want to permanently delete from Time Machine.
  - 4 Click the Action pop-up menu and select "Delete All Backups of *"File or Folder name."*
  - 5 When the warning message appears, click OK to permanently delete the file or folder.
- All backup copies of your file or folder are permanently deleted from your computer.

## Storing Backups Inside Secure Storage

You can also perform backups of specific files or folders that contain sensitive data by placing your data in an encrypted disk image. This image can then be placed on any server that is backed up regularly and still maintain the integrity of your data because it is protected by encryption.

For example, Mac users that are in a Windows Server environment can use this method of backing up to ensure that sensitive data is secure and regularly backed up.

### To securely encrypt and back up data:

- 1 Create a disk image.

For more information about creating a disk image, see “Encrypting Portable Files” on page 143.

- 2 Mount the disk image.
- 3 Copy the files you want to back up onto the disk image.
- 4 Unmount the image and copy it to your backup media.

If you’re in a Windows Server environment, copy your image to a folder that is backed up by the Windows server. Your data will be encrypted and backed up.

## Restoring Backups from Secure Storage

If you accidentally delete or lose a file, you can restore it from your encrypted backup media.

### To restore from your encrypted backup:

- 1 Access the media that contains your disk image backup.
- 2 Mount the disk image and, if prompted, enter your password for the image file.

If the image is on a network, you don’t need to copy it locally. It will securely mount across the network because the data is encrypted.

- 3 Copy the backup of the file you lost locally to your computer.
- 4 Unmount the disk image.

Use this chapter to learn about settings and configurations for network services to improve the security of network communication.

Securely configuring network services is an important step in securing your computer from network attacks.

Organizations depend on network services to communicate with other computers on private networks and wide area networks. Improperly configured network services can provide an avenue for attacks.

## Protecting Data While Using Apple Applications

Although Apple applications are secure by default, you can further enhance security by using the following information.

### Mail Security

You can change Mail preferences to enhance security. Depending on your mail server settings, consider changing Mail preferences so you use SSL and a Kerberos-based authentication method. These settings must match those provided by your mail server.

Only send mail that is digitally signed and encrypted. Digitally signed messages let your recipients verify your identity as the sender and provide assurance that the message was not tampered with in transit. Encrypted messages keep the contents of the message private and readable only by the intended recipient.

You can only send encrypted messages to recipients if you have received a digitally signed message from them or if you have access to their public key. Recipients receive your public key when they receive your signed messages.

This certificate-based system is referred to as public key infrastructure (PKI) messaging. It verifies that the message is from you and that it has not been altered in transit. When you use PKI and encrypt a message, only the intended recipient can read and view its contents.

Mail recognizes sender and recipient certificates. It notifies you of the inclusion of certificates by displaying a Signed (checkmark) icon and an Encrypt (closed lock) icon.

When sending signed or encrypted mail, the sender's certificate must contain the case-sensitive mail address listed in Mail preferences.

To further enhance security, disable the display of remote images in HTML messages in Mail's Viewing preferences. Bulk mailers use image-tracking mechanisms to find individuals who open junk mail. If you don't load remote images, you help reduce spam.

If you use a third-party mail application, consider applying similar security guidelines.

For more information, open Mail Help and search for "security."

## Enabling Account Security

You can configure Mail to send and receive secure mail by using SSL to provide a secure connection to the mail server. Mac OS X version 10.5 Leopard supports SSLv2, SSLv3, and TLSv1. SSL uses public key encryption to provide authentication of the server to the client, and to protect email communications between the machines.

If you are using SSL to connect to your mail server, your password and data are securely transmitted. However, you can further secure your password by using a strong authentication method that provides additional password protection, as well as stronger identity validation. You can protect your password by using one of the following authentication methods:

- MD5 Challenge-Response
- NTLM
- Kerberos Version 5 (GSSAPI)
- Authenticated POP (APOP)

**Note:** Password is the default selection here. Using Password for this option does not provide any additional authentication or password protection.

The authentication method chosen here should match the configuration of the mail server for the account being established. Both the server and the client must be configured with the same authentication method in order to communicate properly.

**To use a secure connection to the mail server:**

- 1 Choose Mail > Preferences and then click Accounts.

2 Select an account and then click Advanced.

3 Select Use SSL.

The port number changes to port 993 for IMAP accounts, and to port 995 for POP accounts. Verify that this port is the same port used by SSL on your mail server. If not, change the port to match the incoming port on the mail server for this account.

4 From the Authentication pop-up menu, select one of the following authentication methods:

- MD5 Challenge-Response
- NTLM
- Kerberos Version 5 (GSSAPI)
- Authenticated POP (APOP)

5 Click Account Information.

6 From the Outgoing Mail Server (SMTP) pop-up menu, select Edit Server List.

7 From the server list, select your outgoing mail server and then click Advanced.

8 Select Secure Socket Layer (SSL).

Verify that this port is the same port used by SSL on your mail server. If not, change the port to match the outgoing port on the mail server for this account.

9 From the Authentication pop-up menu, select one of the following authentication methods:

- MD5 Challenge-Response
- NTLM
- Kerberos Version 5 (GSSAPI)

10 Close the preferences window, and then click Save in the message that appears.

## Remote Content and Hidden Addresses

The above measures provide security while transmitting the messages between the client and the server. These precautions cannot guarantee that the sender is not malicious, however. Users should never open attachments from unknown senders, and should not automatically display remote content from senders without first personally confirming the sender's identity.

An email can be created to display anything in the "To:" line in a graphical, user-friendly application such as Mail. The Mail application default is set to display the user-friendly name rather than the actual email address in the "To:" line of the email display. This should be changed to display the actual email address of the sender instead.

Also, the default is for the Mail application to display remote images in HTML messages. Since these images are displayed immediately, before the user can determine if the sender is known or not, this remote content should not be displayed.



#### To turn off Smart Addresses and remote images:

- 1 Choose Mail > Preferences and then click Viewing.
- 2 Click to disable “Display remote images in HTML messages”.
- 3 Click to disable “Use Smart Addresses”.
- 4 Close the Preferences window.

### Disable the Preview Pane for Mail Messages

In order to completely avoid viewing messages from malicious senders, the message preview pane should be disabled. Once it is disabled, messages will need to be explicitly double-clicked in order to be opened and displayed. Users should then only open messages from known good senders.

#### To disable automatic message viewing:

- 1 Locate the horizontal bar separating the list of email messages and the display of the currently selected email message.
- 2 Double-click the separator bar. It should move to the bottom of the window and remain there.

Once this capability is disabled, the user will need to double-click on each email message individually to open and view it. Any suspicious or unwanted email messages can be deleted without viewing the body of the message.

### Signing and Encrypting Mail Messages

A signed message (including attachments) enables recipients to verify your identity as the sender and provides assurance that your message wasn’t tampered with in transit.



To send a signed message, you must have a digital identity in your keychain. Your digital identity is the combination of a personal certificate and a corresponding private key. You can view digital identities in your keychain by opening Keychain Access and clicking My Certificates in the Category list.

If you only have the certificate portion of your digital identity, you can't send signed messages. You must have the corresponding private key. Also, if people use your certificate to send you an encrypted message, you must have your private key installed on the computer that you are trying to view the message on. Otherwise, you cannot view the encrypted message.

An encrypted message (including attachments) offers a higher level of security than a signed message. To send an encrypted message, you must have a digital identity and the certificate of each recipient must be installed in Keychain Access.

**To sign and encrypt a message:**

- 1 Choose File > New Message and choose the account in the Account pop-up menu for which you have a personal certificate installed in your keychain.

A Signed icon (a checkmark) on the upper right side above the message text indicates the message will be signed when you send it.

- 2 Address the message to recipients.

If you're sending the message to a mailing list, send it unsigned. Many mailing lists reject signed messages (because the signature is an attachment). To send the message unsigned, click the Signed icon. An "x" replaces the checkmark.

An Encrypt (closed lock) icon appears next to the Signed icon if you have a personal certificate for a recipient in your keychain. The icon indicates the message will be encrypted when you send it.

If you don't have a certificate for all recipients, you're asked to cancel the message or send the message unencrypted. To send the message unencrypted, click the Encrypt icon. An open lock icon replaces the closed lock icon.

If your recipients use Mail, security headers marked Signed and Encrypted are visible in the messages they receive. If they're using a mail application that doesn't use signed and encrypted messages, the certificate might be in the form of an attachment. If recipients save the attachment as a file, they can add your certificate to their keychains.

## Web Browsing Security with Safari

You can change Safari preferences to enhance security. By customizing your Safari preferences you can prevent information on your computer or about your computer from being compromised or exposed to an attacker.

In particular, consider changing Safari preferences to disable AutoFill options, to open safe files after downloading, to disable cookies (from sites you navigate to), to disable javascript, and to ask before sending nonsecure forms.

After disabling cookies, remove existing cookies using the Show Cookies dialog in Safari Security preferences. For websites that require cookies, enable cookies and then disable them after visiting the site.

Enabling and disabling cookies can be time-consuming if you visit many sites that use cookies. Consider using multiple accounts with different cookie settings. For example, your personal account might allow all cookies, while your more secure account has restrictive cookie settings.

Javascript has built-in security restrictions that limit javascript applications and prevent them from compromising your computer. However, by disabling it, you can further secure your computer from unauthorized javascript applications attempting to run on your computer.

When using Safari, use private browsing. Private browsing prevents Safari from logging actions, adding webpages to history, keeping items in the Downloads window, saving information for AutoFill, and saving Google searches. You can still use the Back and Forward buttons to navigate through visited sites. After you close the window, the Back and Forward history is removed.

After using Safari, empty the cache. Caching improves performance and reduces network load by storing viewed webpages and webpage content on your local hard disk, but it is a security risk because these files are not removed.

Safari supports server-side and client-side authentication using X.509 certificates. Server-side authentication occurs when you access webpages that use an https URL. When Safari uses client-side authentication, it provides the server with a credential that can be a certificate in your keychain, or it can be from a smart card (which is treated like a keychain).

If you use a third-party web browser, apply similar security guidelines.

For information about how to perform these tasks and for other Safari security tips, open Safari Help and search for “security.”

## Verifying Server Identity

When you receive a certificate from a server, your computer verifies the authenticity of the certificate by checking the signature inside the certificate to determine if it’s from a trusted Certificate Authority (CA).

There are two common methods for verifying the validity of a certificate: Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL).

For a CRL, information about the status of certificates is stored on a revocation server. The Mac OS X security system can check with the revocation server to validate the certificate. The trusted commercial CA certificates are installed on your computer and are used to verify certificates you receive. You can set this in Keychain Access preferences.

You can also visually inspect certificates using Safari or Keychain Access.

To check the validity of a certificate while using Safari, click the lock in the upper right corner of the page. A certificate drop-down page appears and a green check icon indicates that the certificate can be trusted. You can continue to move up the chain of certificates checking their validity and verifying the green check icon is there.

If a certificate is invalid, the lock icon turns red. The invalid certificate has a red-x icon indicating it is invalid.

You can use Certificate Assistant in Keychain Access to evaluate a certificate and determine if it is genuine. Software that uses certificates, such as a mail application or web browser, usually evaluates certificates before using them. However, the Certificate Assistant lets you evaluate certificates given to you with a greater amount of control and detail.

**To visually validate a certificate using Certificate Assistant:**

- 1 Open Keychain Access (located in Applications/Utilities).
- 2 Choose Keychain Access > Certificate Assistant > Open.
- 3 Read the introduction and click Continue.
- 4 Select “View and evaluate certificates” then click Continue.
- 5 Select a trust policy.

For an explanation about the trust policy, click Learn More.

- To evaluate a email certificate, select “S/MIME (Secure Multipurpose Internet Mail Exchange)” and enter the mail address of the sender.
- To evaluate a web server, select “SSL (Secure Socket Layer)” and enter the host server’s URL. If you want to ask the host for the certificates, select “Ask Host For Certificates.”
- For any other type of certificate, select “Generic Apple X509.”

- 6 Click Continue.
- 7 Click the Add (+) button and select the certificate you want to evaluate.

You can add and evaluate multiple certificates.

To include other certificates from your keychain when evaluating the certificate chain, select “Include certificates from my keychain.” For example, if the root and intermediate certificates for your selected certificate are in your keychain, selecting this button includes them in the evaluation.

The default certificate evaluated is always the user certificate, or leaf. If the certificate you want to evaluate is an intermediate or root certificate click Make Leaf.

## Client-Side Authentication

Some applications or services require that you use a digital certificate to authenticate. Digital certificates can be stored in a Smart Card and can also include a photograph of the authorized user to further protect a certificate from being used by an unauthorized user.

By using a certificate as an authentication and identification method, the service or application can ensure that the person who provided the certificate is not only the same person who provided the data, but is also who they say they are. The certificate is also signed—in this case by the certificate authority (CA) who issued the certificate.

## Managing Data Communication and Execution

Downloaded files are tagged with the `com.apple.quarantine` extended attribute until you permit the file to be opened or executed.

### Opening Safe Files

When you enable “Open ‘safe’ files after downloading” in Safari preferences, files that are considered safe are opened after downloading. These include pictures, movies, sounds, text files, PDFs, disk images, and ZIP archives.

Before they are opened, the following content factors are examined to verify that the file is safe:

- The file extension
- The MIME type
- What’s inside the file

Sometimes malware tries to disguise itself as safe, but Mac OS X Leopard checks for signs that indicate this. If Safari considers that a downloaded file is safe:

- Safari opens the file after it downloads.
- If the downloaded file is an archive (.zip file), Safari decompresses it.
- If the downloaded file is a disk image (.img file), Safari mounts the image volume.

Other types of files might not be safe. Applications, scripts, web archives, and archives that contain applications or scripts can harm your computer. Not all such files are unsafe, but you should exercise caution when opening a downloaded file.

**Note:** Although Safari, iChat, and Mail offer Download Validation for increased security, no software can detect all potentially dangerous file types.

If Download Validation determines that a downloaded file is unsafe, you are prompted to download or cancel the download. If you download the file, it is placed in your download location as configured in Safari preferences. If you cancel, the file is not saved.

If Download Validation cannot determine that a downloaded file is safe, it is stored in your default download directory in the same way it is if the "Open 'safe' files after downloading" preference was disabled.

The file is named the same as the original file with ".download" at the end of it. This can be moved to the Trash or inspected manually.

## Nonsecure Forms

In some cases, forms you complete in Safari might be submitted in a nonsecure way to a secure website. Safari is set to display a message when this is about to happen, so you can prevent the form from being submitted if you are concerned about the security of your information.

If you don't want to see this message, choose Preferences from the Safari menu and click Security. Deselect the checkbox labeled "Ask before sending a nonsecure form to a secure website."

## Syncing Bookmarks

If you're using Mac OS X Leopard or later and Safari 1.0 or later, you can synchronize your Safari bookmarks with the bookmarks in your MobileMe Bookmarks library on the web. You can also synchronize your Safari bookmarks across multiple Mac OS X computers.

With bookmark synchronization turned on, the bookmarks in your MobileMe Bookmarks application on the web synchronize with Safari on your computer's hard disk each time you sync. (After you sync, it might take a few minutes before you see the changes.)

You can turn off synchronization in Safari preferences by deselecting "Turn on MobileMe Bookmarks Synchronization." While synchronization is off, changes you make to bookmarks in MobileMe Bookmarks or Safari are saved until the next time you turn on synchronization and click the Sync Now button in the MobileMe pane of System Preferences (Mac OS X version 10.4 Tiger or later) or in iSync.

For example, if you delete a bookmark from MobileMe Bookmarks with synchronization turned off, the bookmark is deleted from Safari on your computer's hard disk the next time you use iSync with synchronization turned on.

## AutoFill

Safari can use information from various sources to complete forms that are on many webpages:

- Personal information, such as mailing addresses, mail addresses, and phone numbers, are retrieved from your Address Book card.
- User names and passwords that you enter on websites are saved in your keychain and retrieved when you try to log in later. (Some websites do not allow you to save your user name and password.)
- Any other information that you enter at a website is saved in Safari's cache to be reused later.

You can select the information that Safari uses to complete web forms. Choose Preferences from the Safari menu and click AutoFill. Then select the items you want Safari to use.

To complete a web form, open the webpage and click the AutoFill button in the address bar. If you don't see the AutoFill button in the address bar, choose AutoFill from the View menu. Items that are completed using AutoFill appear in yellow in the webpage.

To complete individual fields in a form, select a text box and start typing. If Safari matches saved information for the field, it finishes entering the text for you. If several items match what you typed, a menu appears. Press the arrow keys to select the correct item and press Return.

Website forms can include items that Safari doesn't recognize. You must fill out these items yourself.

If you enter a user name and password, Safari asks if you want to save the information. Click Yes to save the name and password. Click Not Now if you want to save the information in the future. Click Never for this Website if you don't want to be asked to save the name and password for the website again.

To change or delete saved user names and passwords or other information, click the Edit button next to the related checkbox in the AutoFill preferences pane.

## Controlling Web Content

A plug-in is software installed on your computer that provides additional capabilities to applications. Safari uses plug-ins to handle multimedia content on webpages, such as pictures, music, and video. For example, the QuickTime Internet plug-in allows Safari to display media content. To see the plug-ins available to Safari, choose Installed Plug-ins from the Help menu.

Some webpages display pop-up windows. For example, a webpage might use a pop-up window to request your user name or to display ads. To block these pop-up windows, choose Safari > Block Pop-Up Windows so that a checkmark appears next to it.

Blocking pop-up windows stops windows that appear when you open or close a page. It does not block pop-up windows that open when you click a link.

If you block pop-up windows, you might miss important information for a webpage.

## Cookie Storage or Tracking Information

A cookie is a small file created by a website to store information. The cookie is stored on your computer. Cookies are normally helpful and harmless. It's rare to encounter a bad cookie.

When you visit a website that uses cookies, the site asks Safari to put cookies on your computer. When you return to the site later, Safari sends back the cookies that belong to the site. The cookies tell the site who you are, so the site can show you information that's appropriate for you.

Cookies store information that identifies you, such as your user ID for a website and your website preferences. A website has access only to the information you provide. A website can't determine your mail address unless you provide it. A website can't gain access to other information on your computer.

When you use the default cookie preferences in Safari, you won't know when Safari is accepting or sending cookies. You can change your cookies preferences so that Safari doesn't accept cookies or so it accepts them only from limited sources.

## Advanced Settings

Use the Advanced preference pane to customize Safari for Universal Access, to customize the appearance of webpages with your own style sheet, and to set proxy settings. You can select from the following:

- The "Never use font sizes smaller than" option prevents text from getting so small that you can no longer read it.
- The "Press Tab to highlight each item on a webpage" option helps you find all links and options on a page by highlighting each one in turn when you press the Tab key.

- The Style Sheet pop-up menu lets you customize the appearance of webpages by selecting a style sheet you've created.
- The Proxies option opens the Network panel in System Preferences so you can edit proxy settings for your current network location.

## Securing File Downloads

If you navigate to a downloadable file with Safari (for example, by clicking a download link), Mac OS X provides download validation to warn you about unsafe file types. Cancel the download if you have doubts about the integrity of the file.

If you download a file by Command-clicking or selecting Download Linked File from a contextual menu, the download is not inspected by the Mac OS X download validation, and it is not opened. Inspect the downloaded file using the Finder. If you were expecting a document and Finder indicates that it is an application, do not open the file. Instead, delete it immediately.

When distinguishing between legitimate and malicious applications, where you get the file from is the most important indicator. Only download and install applications from trusted sources, such as well-known application publishers, authorized resellers, or other well-known distributors. Use antivirus software to scan files before installing them. A selection of third-party products is available at the Macintosh Products Guide.

## Instant Message Security with iChat AV

Although iChat can be configured to be used with security, disable it unless your organization requires messaging services.

You can set up secure iChat messaging using your MobileMe membership. However, both you and your iChat buddy must be MobileMe members and have Mac OS X version 10.4.3 Tiger or later installed. With a MobileMe membership, you can sign up for a Secure iChat certificate that allows you to enable secure messaging.

Also, if you are not able to use MobileMe you can create a certificate using Certificate Assistant. You can use that certificate to encrypt the iChat AV communication without using a MobileMe account. For more information about creating a certificate, see "Creating a Self-signed Certificate" on page 83.

When you enable iChat encryption, iChat performs a Certificate Signing Request (CSR) to MobileMe. iChat then receives a certificate, which includes your original public key and a private key. The public and private key pair is created by the CSR process.

iChat AV Encryption leverages a PKI approach. The public and private asymmetric keys are derived from the user's MobileMe identity, which consists of the user's certificate and private key. The private key and certificate represent your MobileMe identity. These keys are used to encrypt content between you and your buddy.



When you securely send a message, iChat requests your buddy's Secure iChat public key. It then encrypts the message based on your buddy's public key. It sends that encrypted message to your buddy, who decrypts the message based on his or her private key.

If your organization runs an internal iChat server, the server can use SSL to certify the identity of the server and establish secure, encrypted data exchange between an iChat user and the server. Consider only accepting messages from specific people or from people on your buddy list. This helps prevent information phishing through iChat.

For more information, open iChat Help and search for "security." For information about iChat and SSL, see *Web Technologies Administration*.

## iChat AV Security

When you share your screen with an iChat buddy, the buddy has the same access to your computer that you have. Share your screen only with trusted parties, and be particularly careful if you receive a request to share your screen from someone who isn't on your buddy list.

If the request comes from someone in your Bonjour list, remember that the person's name is not necessarily accurate, so his or her identity is uncertain.

Although every screen-sharing connection uses encryption, the highest level of security requires both participants to have MobileMe accounts with encryption enabled or a certificate created by Certificate Assistant. If this is the case, you will see a lock icon in the screen-sharing window. To quickly end a screen-sharing session, press Control-Escape.

iChat AV in Mac OS X version 10.4.3 Tiger and later encrypts all communications between MobileMe members and certificate users. Text messages, audio chats, video conferences, and file transfers are secured using robust 128-bit encryption so that others can't eavesdrop on your communications.

If you have an active MobileMe account, you can set up iChat to encrypt communications when you chat, conference, or send files to other MobileMe members who have set up iChat encryption.

## Enabling Privacy

To prevent messages temporarily, set your status to Offline or Invisible, or log out by choosing iChat > Log Out.

You can also specify that messages from specific people be blocked or allowed. Blocked people can't send you messages or see when you are online.

### To block people:

- 1 Choose iChat > Preferences and then click Accounts.

- 2 Select the account you want to set privacy options for.

Bonjour and Jabber accounts don't have privacy options.

- 3 Click Security.
- 4 From the Privacy Level list, select an option.

If you select "Allow specific people," click the Edit List button, click the Add (+) button, and then enter the names or IDs for those you want to allow. Anyone not added to the list is blocked.

If you select "Block specific people," click the Edit List button, click the Add (+) button, and then enter the names or IDs for those you want to block. Anyone not on the list is allowed.

To quickly add a person to the list of blocked people, click the Block button that appears in the message window when you get a message from that person.

You can't see or send messages to people you have blocked.

### Enabling Encryption Using MobileMe Identity

You can secure your iChat communications so no one can access your conferences. To use this safeguard, you and your iChat buddy must both have MobileMe accounts and request MobileMe identity certificates.

#### To set up secure messaging:

- 1 Choose iChat > Preferences and then click Accounts.
- 2 Select the MobileMe account you want to secure.

Free trial MobileMe memberships are not eligible for secure messaging.

- 3 Click Security and then click Encrypt.

As part of the setup process, you must enter a MobileMe account password. This is the password you enter if you are using secure messaging on a second computer. This password must be different from your Mac OS X password.

When you and your buddy have the MobileMe certificate installed and you start a chat, a lock icon appears in the upper-right corner of the iChat window. Text, audio, and video are encrypted on your computer and are not decrypted until they reach your buddy's computer.

To view your Secure iChat certificate, open Keychain Access and click My Certificates in the Categories window. Double-click the certificate that matches your MobileMe short name.

## Multimedia Security with iTunes

Your iTunes account is protected by your user name and password, which should never be shared with other users, to prevent it from being compromised by an unauthorized user. If an unauthorized user gains access to your user name and password, they can use your account to purchase music, videos, and podcasts from the iTunes store.

You can protect your iTunes account from being compromised by using a strong password. When creating your iTunes password, use Password Assistant to help you generate a strong password.

Also, you can use the sharing preference of iTunes to share your music with other network users. When configuring iTunes sharing preference, require that users set a strong password to access your shared music. You can generate a strong password using Password Assistant. When you finish sharing your music, turn the iTunes sharing preference off to keep unauthorized users from attempting to access your shared iTunes music.

For more information about creating strong passwords, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.

## Guest Operating Systems with Boot Camp

With Boot Camp you can install and run other operating systems such as Windows XP or Windows Vista on your Intel-based Mac computer.

Boot Camp Assistant (located in /Applications/Utilities) helps you set up a Windows partition on your computer's hard disk and then start the installation of your Windows software.

When you install a guest operating system on your Intel-based Mac computer, access control lists (ACLs) set on your Mac partition might not be enforced by the guest operating system. This creates a possible point of intrusion or corruption to your sensitive data. When the guest operating system is booted, your computer becomes susceptible to network vulnerabilities of the guest operating system.

If you decide to use a guest operating system on your Mac computer, use encrypted disk images to store your data when you are using Mac OS X. This prevents your sensitive data from being accessed by the guest operating system. For more information, see “Creating an Encrypted Disk Image” on page 143.

Also, keep backup copies of your data in the event that your Mac OS X partition becomes corrupt.

When setting a password for your guest operating system, start in Mac OS X Leopard and use Password Assistant to create a strong password. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.

You can also prevent attacks by keeping your guest operating system installed with the most current updates.

## Protecting Data While Using Apple Services

You can protect your data when sending it across unsecure networks, such as the Internet, by using a secure network connection. This prevents unauthorized access to your data.

## Securing Remote Access Communication

You can secure remote access to other networks by using a Virtual Private Network (VPN). A VPN consists of computers or networks (nodes) connected by a private link that transmits encrypted data. This link simulates a local connection, as if the remote computer were attached to the local area network (LAN).

VPN is the tunnel mode of the IPSec protocol, which is a collection of protocols used to secure Internet Protocol (IP). IPSec encrypts the data transmitted over IP.

## VPN Security (L2TP and PPTP)

There are two encrypted transport protocols: Layer Two Tunneling Protocol, Secure Internet Protocol (L2TP/IPSec) and Point-to-Point Tunneling Protocol (PPTP). You can enable either or both of these protocols. Each has its own strengths and requirements.

The L2TP over IPSec protocol provides the highest level of security because it runs over IPSec. PPTP does not use the IPSec protocol, which makes it a less secure VPN protocol.

## L2TP over IPSec

L2TP is an extension of PPTP used by Internet service providers to enable a VPN over the Internet. IPSec is a set of security protocols. When you combine IPSEC with LT2P, IPSec encrypts the data to ensure data integrity and L2TP creates the tunnel for the data to be transferred.

L2TP/IPSec uses strong IPSec encryption to tunnel data to and from network nodes. It is based on Cisco's L2F protocol.

IPSec requires security certificates (self-signed or signed by a CA such as Verisign) or a predefined shared secret between connecting nodes. The shared secret must be entered on the server and the client.

The shared secret is not a password for authentication, nor does it generate encryption keys to establish secure tunnels between nodes. It is a token that the key management systems use to trust each other.

L2TP is Mac OS X Server's preferred VPN protocol because it has superior transport encryption and can be authenticated using Kerberos.

## IPSec Configuration

Mac OS X Leopard computers can be configured to use DHCP to obtain IP addresses and retrieve information about an LDAP directory from the DHCP server. After you configure the DHCP service with information about an LDAP directory, that information is delivered to Mac OS X clients when they receive IP addresses from the DHCP server. If necessary, configure Mac OS X clients to retrieve information from the DHCP server.

The following settings are configured:

- Network preferences are set to use DHCP. To access the setting, select System Preferences, open Network preferences, select the internal Ethernet interface, and select “Using DHCP with manual address” or “Using DHCP” from the Configure IPv4 pop-up menu.
- The computer’s search policy is set to be defined automatically. To access this setting, open Directory Utility (in /Applications/Utilities/) and click Search Policy, then click Authentication. If the lock icon is locked, click it and authenticate as an administrator. Choose Automatic from the Search pop-up menu, then click Apply.
- The use of DHCP-supplied LDAP information is enabled. To access this setting, open Directory Utility and click Services. If the lock icon is locked, click it and authenticate as an administrator. Select LDAPv3 in the list of services, then click Configure. Click “Use DHCP-supplied LDAP Server,” then click OK.

### To configure Mac OS X clients so they can use the VPN server:

- 1 Open System Preferences, then click Network.
- 2 Click the Add (+) button at the bottom of the network connection services list and then choose VPN from the Interface pop-up menu.
- 3 From the VPN Type pop-up menu, choose “L2TP over IPsec” or “PPTP” according to your network.
- 4 Enter a VPN service name in the Service Name field, then click Create.
- 5 Enter the DNS name or IP address in the Server Address field.  
Server Address: gateway.example.com
- 6 Enter the user account name in the Account Name field.  
Account Name: *<the user’s short name>*
- 7 Click Authentication Settings and enter the User Authentication and Machine Authentication configuration information.
- 8 Click OK.

## Understanding PPTP

PPTP is a commonly used Windows standard VPN protocol. PPTP offers 128 bit encryption (if strong passwords are used) and supports a number of authentication schemes. It uses a user-provided password to produce an encryption key.

By default, PPTP supports 128-bit (strong) encryption. PPTP also supports the 40-bit (weak) security encryption.

## Network Access Control (802.1x)

AirPort or Ethernet networks can be protected by the Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard. The 802.1x standard enhances the security of a LAN.

802.1x is used to protect your network from unauthorized users that attempt to attach to your wireless or wired network LAN. Mac OS X Leopard also provides multidomain 802.1x support for Login Window domains, User domains, and System domains. You can only enable and use one of these. For example, you cannot combine User and System domain. To configure the settings for 802.1x, use Network preferences.

## Securing Internet Communication with Host-Based Firewalls

Using a firewall to filter network traffic from a host or a network of hosts that are attempting to access your computer, prevents attackers from gaining access to your computer.

### Firewall Protection

A Firewall is software that protects your Mac OS X computer from unauthorized users. When you turn firewall protection on, it is similar to erecting a wall to limit access to your computer. The firewall scans incoming network traffic and rejects or accepts these packets based on rules. You can restrict access to any network service running on your computer.

You can monitor activity involving your firewall by enabling firewall logging. Firewall logging creates a log file that tracks activity such as the sources and connection attempts blocked by the firewall. You can view this log in the Console utility.

Mac OS X includes two firewalls: the Application Firewall and the IPFW firewall. If you turn on a sharing service, such as file sharing, Mac OS X's Application Firewall uses code-signing technology to verify that the program has been signed by Apple and allows it to use the network.

In addition to the sharing services you turn on in Sharing preferences, the list can include other services, applications, and programs that are allowed to accept network connections. An application or program might have requested and been given access through the firewall, or it might be signed by a trusted certificate and therefore allowed access.

**Important:** Some programs have access through the firewall although they don't appear in the list. These might include system applications, services, and processes. They can also include digitally signed programs that are opened by other programs. You might be able to block these programs' access through the firewall by adding them to the list.

To add an application to the list, select "Set access for specific services and applications" in the Firewall pane of Security preferences, click Add (+) at the bottom of the list, and then select what you want to add. After the program is added, click the up and down arrows to allow or block connections through the firewall.

**Note:** Blocking a program's access through the firewall might harm the program or other programs that depend on it, or it might affect the performance of other applications and services you use.

When the system detects a connection attempt to a program that is not enabled in Security preferences or is not signed, you are prompted to allow or deny access to the program. If you don't respond, the program is added to the list in the Firewall pane of Security preferences and the access is set to "Allow only essential services."

## The Application Firewall

Mac OS X Leopard or later includes a new technology called the Application firewall. This type of firewall permits you to control connections on a per-application basis, rather than a per-port basis.

The Application firewall makes it easier for users to gain the benefits of firewall protection and helps prevent undesirable applications from taking control of network ports that should only be used by legitimate applications.

The firewall applies to TCP and UDP, the Internet protocols most commonly used by applications. It does not affect AppleTalk. The system can be set to block incoming ICMP pings by enabling Stealth Mode in Advanced settings.

Earlier IPFW technology is still accessible from the command line (in Terminal), and the Application firewall doesn't override rules set with IPFW. If IPFW blocks an incoming packet, the Application firewall does not process it.

## Application Firewall Architecture

The Application firewall has the following modes of operation:

- *Allowing all incoming connections:* This is the most open mode. Mac OS X does not block incoming connections to your computer. This is the default mode for Mac OS X Leopard. If you upgraded from Mac OS X Tiger, your Application firewall defaults to this mode.

- *Allow only essential services:* This is the most conservative mode. Mac OS X blocks all incoming connections except a limited list of services essential to operating your computer and those services that have been activated in the Sharing Preference pane. The system services that are still allowed to receive incoming connections are:
  - **configd:** Implements DHCP and other network configuration services.
  - **mDNSResponder:** Implements Bonjour.
  - **racoon:** Implements Internet Key Exchange (IKE).
- *Set access for specific services and applications:* This mode offers you the most flexibility. You can choose whether to allow or deny incoming connections for any application on your system. After you add an application to the list, you can choose whether to allow or deny incoming connections for that application. You can even add command-line applications to this list.

When you add an application to this list, Mac OS X digitally signs the application (if it has not been signed). If the application is later modified, you are prompted to allow or deny incoming network connections to it. Most applications do not modify themselves. This is a safety feature that notifies you of the change.

## Enabling Advanced Features

The Application Firewall has the following advanced features that can be used to log firewall activity and hide the computer from unwanted network scans (ICMP).

## Firewall Logging

You can monitor firewall activity by enabling firewall logging. Firewall logging creates a log file that tracks activity such as the sources and connection attempts blocked by the firewall. You can view this log in the Console utility.

### To enable firewall logging:

- 1 Open System Preferences.
- 2 Click Security and then click Firewall.
- 3 Open the Firewall pane of Security preferences  
If some settings are dimmed, click the lock icon and enter an administrator name and password.
- 4 Click Advanced.
- 5 Select the Enable Firewall Logging checkbox.
- 6 To view firewall activity, click Open Log.

## Stealth Mode

Computer hackers scan networks so they can attempt to identify computers to attack. You can prevent your computer from responding to some of these scans by using Stealth Mode.



When Stealth Mode is enabled, your computer does not respond to ICMP ping requests, and does not answer to connection attempts from a closed TCP or UDP port. This makes it more difficult for attackers to find your computer.

**To enable stealth mode:**

- 1 Open System Preferences.
- 2 Click Security and then click Firewall.
- 3 Open the Firewall pane of Security preferences.

If some settings are dimmed, click the lock icon and enter an administrator name and password.

- 4 Click Advanced.
- 5 Select the Enable Stealth Mode checkbox.

## Protection from Unauthorized Applications

Applications not in the list that have been digitally signed by a CA trusted by the system (for the purpose of code signing) can receive incoming connections. Every Apple application in Mac OS X Leopard has been signed by Apple and can receive incoming connections. To deny a digitally signed application, add it to the list and then explicitly deny it.

If you run an unsigned application not in the Application firewall list, you must allow or deny connections for the application using the dialog. If you choose Allow, Mac OS X Leopard signs the application and adds it to the Application firewall list. If you choose Deny, Mac OS X Leopard signs the application, adds it to the Application Firewall list, and denies the connection.

Some applications check their own integrity when they are run without using code-signing. If the Application firewall recognizes the application, it does not sign the application. Instead, it displays the dialog every time the application runs. To prevent this dialog from appearing, upgrade to a version of the application that is signed by its developer.

Some harmful applications can cause problems for your computer. Frequently, a harmful application tries to appear as an innocent document, such as a movie or graphic file. These applications, called trojans, are most often spread by Internet downloads and mail enclosures.

**Important:** If you receive an application warning and you don't expect the file to be an application, don't open the file. Delete it from your computer.

**To protect your computer from harmful applications:**

- Accept applications only from known and trusted sources.
- Run an antivirus program if you find suspicious files or applications, or if you notice unusual behavior on your computer.

- To reduce the amount of exposure to harmful applications or files, limit the number of administrator accounts you create. Consider creating a user account for your daily work and then use an administrator account only when you need to install software or administer accounts.
- If you enabled the root user and you don't need it, disable it.

## The IPFW2 Firewall

Mac OS X Leopard includes the open source IPFW2 software as an alternate firewall. You use the `ipfw` command-line tool to filter packets by using rules to decide which packets to allow and which to deny.

The firewall scans incoming IP packets and rejects or accepts them based on the set of filters or rules you create. You can restrict access to any IP service running on your computer, and you can customize filters for all incoming addresses or for a range of IP addresses.

IPFW handles packets at a lower level of the networking stack than the Application firewall. Therefore, its rules take precedence over the Application firewall.

## Configuring the IPFW Firewall

The IPFW2 firewall (also referred to here as IPFW) allows for the creation of complex and powerful packet filtering rulesets. This firewall can be difficult to configure, and can also disrupt network communications if improperly configured. It requires manually written rules, and the system must be configured to read those rules at startup. Configuring IPFW rulesets requires a higher level of expertise than many system administration tasks. If an administrator is not mindful of the IPFW ruleset on the system, confusion can arise when some network connectivity is not available that apparently should be.

## Understanding IPFW Rulesets

An IPFW configuration or ruleset is a list of rules that are designed to match packets and take appropriate action. IPFW rules are numbered from 1 to 65535. The packet passed to the firewall is compared against each of the rules (in numerical order). When the packet matches a rule, the corresponding action is taken. A more complete description of the capabilities and configuration of IPFW can be found in the `ipfw` man page.

To view the currently enforced IPFW rules, run the command:

```
$ sudo ipfw print
```

The default output should appear something like this:

```
65535 allow ip from any to any
```

This line shows that the default configuration allows all traffic through the IPFW firewall, performing no filtering. Like all IPFW rules, it consists of a rule number (65535); an action (allow); and body (ip from any to any). In this case, the body (ip from any to any) matches all IP packets. This also happens to be a special rule, called the default rule. It is the highest-numbered rule possible and is compiled directly into the kernel. Because no rules have actually been added to the system, all packets are passed to this default rule, which allows them all through. However, if the Stealth Mode feature is enabled on the system, then the following line will appear first in the list:

```
33300 deny icmp from any to me in icmp types 8
```

This rule shows the implementation of the Stealth Mode feature: dropping any incoming ping echo requests, which is ICMP type 8. Because it is a lower rule number (and thus also appears earlier when listed), it is consulted before the default rule.

With the exception of the Stealth Mode blocking of ping requests, the default configuration for IPFW on Mac OS X does not block any packets. Mac OS X relies primarily on the Application firewall to block unwanted network traffic. IPFW can be used to write complex and powerful rulesets, which make decisions about connectivity based on the form of the packet. The Application Firewall, on the other hand, makes decisions about connectivity based on whether the program trying to use the network is trusted. These two firewall technologies complement each other.

The next section describes how to make use of IPFW.

## Implementing an IPFW Ruleset

Implementing an IPFW ruleset can be a challenging activity, filled with corner cases and problems that are difficult to debug. Because of this, administrators should develop a thorough understanding of a simple, strict ruleset and then carefully modify it to suit the needs of their particular network environment. This section first describes how to enable logging so that debugging is possible. Next, a simple ruleset is provided, and then ways in which it can be expanded are presented.

### Enabling Firewall Logging

Even before implementing an IPFW ruleset, firewall logging should be enabled. This can be performed in the Security pane of System Preferences, and is described in the Firewall Settings section of “Securing Security Preferences.” This setting enables logging for both the Application firewall and IPFW.

The system's ability to log packets can then be verified with the following command:

```
$ sudo sysctl net.inet.ip.fw.verbose
```

If the command returns a 2, then logging is enabled for both the Application firewall and IPFW. The system should now send both Application firewall and IPFW log messages to `/var/log/appfirewall.log`. These can be viewed using the Console program in `/Applications/Utilities`. Implementation of a basic ruleset can proceed, using the log to debug any connectivity failures that occur.

### Implementing a Basic Inclusive Ruleset

An IPFW ruleset can be stored simply as a list of IPFW rules inside a text file. Traditionally, the file `/etc/ipfw.conf` is used to store these rules. Proper firewall ruleset design is inclusive: it allows only packets that match specific rules, and then denies all others. The following basic ruleset is inclusive and also very strict: it allows packets from other systems only when the host has initiated a connection to another system. This is appropriate for a client system that offers no network services to any other systems.

To implement this ruleset, enter the following rule in `/etc/ipfw.conf` file:

```
#Allow all traffic to us from our loopback interface
add 1000 allow all from any to any via lo0
#Allow all TCP packets out, and keep state in order to allow responses
add 10000 allow tcp from any to any out keep-state
#Allow all UDP packets out, and keep state in order to allow responses
add 12000 allow udp from any to any out keep-state
#Allow all ICMP traffic
add 20000 allow log icmp from any to any
#Allow DHCP packets in (use only if using DHCP)
add 60000 allow udp from any to any src-port 67 dst-port 68 in
#Reject all IP packets: anything not matched already will be dropped and
    logged
add 65534 deny log ip from any to any
#Allow all IP packets: here as a comment as a reminder of the default rule
#65535 allow ip from any to any
```

Once this ruleset is in `/etc/ipfw.conf`, it can be loaded with the command:

```
$ sudo /sbin/ipfw /etc/ipfw.conf
```

The following command can be issued to verify that the rules are loaded as expected:

```
$ sudo /sbin/ipfw print
```

Testing can now commence to determine whether the ruleset is compatible with your connectivity needs. If modifications are made to the ruleset in the file, the old rules must be flushed before your new rules are inserted. To flush the old rules and then re-insert a ruleset from `/etc/ipfw.conf`:

```
$ sudo /sbin/ipfw flush
$ sudo /sbin/ipfw /etc/ipfw.conf
```

Be sure to read the later section which describes the steps necessary to ensure that the rules in `/etc/ipfw.conf` are loaded at startup. Even if DHCP is not used, any unconnected interfaces may create log messages when they attempt to obtain IP settings from the computer. To eliminate these messages, configure those interfaces to "Off" using the Network preference pane.

### Opening the Basic Ruleset to Permit Services

The basic ruleset described earlier does not permit the system to host any network services, such as Bonjour or Remote Login (SSH). This section describes rules that can be added to the firewall to allow the system to host some network services. Each of these rules should only be added if the system truly needs to offer the network service discussed. All possible network services cannot be covered here, but rules to allow other services should be available from other resources.

Add the following rules to allow Bonjour, substituting your local network and netmask for `a.b.c.d/nm`:

```
add 12600 allow udp from a.b.c.d/nm to any dst-port 5353
add 12601 allow udp from a.b.c.d/nm 5353 to any dst-port 1024-65535 in
```

Add the following rules to allow the Remote Login (SSH) service to be reached, substituting `a.b.c.d/nm` for networks you wish to allow:

```
add 12500 allow tcp from a.b.c.d/nm to any 22
add 12501 allow udp from a.b.c.d/nm to any 22
```

Add the following rules to allow the system to host File Sharing over AFP, substituting `a.b.c.d/nm` for networks you wish to allow:

```
add 12700 allow tcp from a.b.c.d/nm to any dst-port 548
```

Add the following rules to allow the Web Sharing service, substituting `a.b.c.d/nm` for networks you wish to allow:

```
add 14000 allow tcp from a.b.c.d/nm to any dst-port 80
add 14000 allow tcp from a.b.c.d/nm to any dst-port 443
```

Add the following rules to allow File Sharing over SMB, substituting your local network and netmask for `a.b.c.d/nm`:

```
add 12801 allow udp from a.b.c.d/nm 137,138,139 to me in keep-state
add 12803 allow tcp from a.b.c.d/nm 137,138,139 to me keep-state setup
```

### Making the Basic Ruleset More Restrictive

The basic ruleset described earlier can be made more restrictive by making it specifically drop some types of packets.

To deny traffic addressed for the loopback interface but not originating from it (must be numbered after rule 1000 above):

```
add 1010 deny all from any to 127.0.0.0/8
```

To restrict ICMP traffic, you must remove rule 20000 above, which accepts all ICMP packets, and then choose which types of ICMP packets to allow. Some ICMP types such as those for message redirection and router solicitation are not typically needed. The following ICMP types are frequently judged necessary for network operation, and all other ICMP types are then denied:

```
# to allow destination unreachable messages
add 20001 allow icmp from any to any icmptypes 3
# to allow source quench / congestion control messages
add 20002 allow icmp from any to any icmptypes 4
# Allow ping responses (echo replies) in
add 20004 allow icmp from any to any icmptypes 0 in
# Allow "time exceeded" responses -- lets traceroute work
add 20005 allow icmp from any to any icmptypes 11 in
```

Removing rule 20000 and adding the rules above effectively enables Stealth Mode, since ICMP message of type 8 are implicitly denied (since they are not accepted). However, it may be necessary to allow ping responses to other systems on the local network but not from elsewhere. To do so, add a rule as follows, substituting your network/netmask for a.b.c.d/nm:

```
add 20010 allow icmp from a.b.c.d/nm to any icmptypes 8 in
```

**Note:** If Stealth Mode is enabled using the Security preference pane, the rule here will take precedence because has a lower number (20010) than the system applies for Stealth Mode (33000).

Packet fragmentation can be normal in some network environments. However, if your network environment should not result in packet fragmentation, then fragmented packets may be a sign of abnormal activity. The following rule will drop any fragmented packets:

```
add 700 deny log ip from any to any frag
```

## Configuring the System to Load the IPFW Ruleset

The system must be configured to automatically load your IPFW ruleset in `/etc/ipfw.conf` at startup.

To do so, create the file `/Library/LaunchDaemons/ipfw.plist` so that it reads as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://
    www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>ipfw</string>
    <key>Program</key>
    <string>/sbin/ipfw</string>
    <key>ProgramArguments</key>
    <array>
        <string>/sbin/ipfw</string>
        <string>/etc/ipfw.conf</string>
    </array>
    <key>RunAtLoad</key>
    <true />
</dict>
</plist>
```

On the next reboot, the IPFW rules in `/etc/ipfw.conf` will be loaded automatically.





Use this chapter to secure network and shared services.

Securely configuring network services is an important step in securing your computer from network attacks.

Organizations depend on network services to communicate with other computers on private networks and wide area networks. Improperly configured network services provide an avenue for attacks.

## Securing Local Services

Your Mac OS X version 10.5 Leopard computer offers many services that can be quickly set up and configured. Although these services are helpful and easy to configure, they must be securely configured to prevent unauthorized users from accessing your computer. Most services can be securely configured by using strong passwords or by turning the services off when they are not in use.

### Securing Bonjour (mDNS)

Bonjour is a protocol for discovering file, print, chat, music sharing, and other services on IP networks. Bonjour listens for service inquiries from other computers and provides information about available services. Users and applications on your local network can use Bonjour to quickly determine which services are available on your computer, and you can use it to determine which services are available on theirs.

This easy exchange of information makes service discovery very convenient, but it also incurs a security risk. Bonjour broadcasts the services that are present and the services you have available. These risks must be weighed against the utility of running a network service such as Bonjour.

Aside from the information freely exchanged by Bonjour, network services inherently incur a security risk due to the potential for implementation errors to allow remote attackers access to your system. However, Bonjour mitigates these risks by implementing sandboxing.

To reduce the security risk of running Bonjour, you should connect only to secure, trusted local networks. You should also verify that Network preferences enables only required networking connections. This reduces the chance of connecting to an insecure network.

Before using Bonjour to connect to a service, verify that the service is legitimate and not spoofed. If you connect to a spoofed service, you might download malicious files.

**Important:** If you cannot trust all services on your local network, then Bonjour should not be used.

To disable Bonjour, enter the following commands:

```
$ sudo launchctl unload -w /System/Library/LaunchDaemons/ \
    com.apple.mDNSResponder.plist
$ sudo launchctl unload -w /System/Library/LaunchDaemons/ \
    com.apple.mDNSResponderHelper.plist
```

If Bonjour is disabled, you must manually configure network printers. Disabling Bonjour can also disable functionality in other applications that rely on Bonjour or possibly make them unusable. For example, there might be issues with calendar and address book sharing, and finding iChat buddies.

If disabling Bonjour interferes with other applications that are absolutely needed by the user, enter the following commands to reenab Bonjour:

```
$ sudo launchctl load -w /System/Library/LaunchDaemons/ \
    com.apple.mDNSResponder.plist
$ sudo launchctl load -w /System/Library/LaunchDaemons/ \
    com.apple.mDNSResponderHelper.plist
```

If you decide to reenab Bonjour, block UDP port 5353 on your firewall to block external Bonjour traffic.

## Securing Application Use of Bonjour

Some applications can be used to share data such as contact information, photos, and music. When these application share your data, they use Bonjour to let other network users know what you are sharing. When you are sharing information, use Password Assistant to help you create a strong password.

## Address Book

You can use your MobileMe account to share your address book with others over the Internet. In Address Book preferences under Sharing, you can add contacts that have a MobileMe account to the sharing list and assign them editing or viewing privileges for your contacts.

When delegating privileges, limit the number of people who have editing privileges. This prevents users from accidentally removing contact information. When your address book is not being used, turn Address book sharing off.

### iChat AV

You can use iChat to communicate with other iChat users that are members of the same iChat server. iChat uses Bonjour to find other iChat instances on your local network. To secure iChat, turn off all Bonjour preferences and use a secure iChat server.

If a request comes from someone in your Bonjour list, remember that the person's name is not necessarily accurate, so his or her identity is uncertain. To prevent unauthorized users from instant messaging you, you can reject their request to send you messages.

### iPhoto

You can share your photos using the sharing pane of iPhoto. Before you begin sharing photos, make sure you are in a trusted or secure environment. To securely share photos, never use your name or user name as the shared name for your photos, and require that viewers use a password to view your photos. When creating the password for viewers, use Password Assistant to help you create a strong password.

### iTunes

You can share your music using the sharing pane of iTunes. Before you begin sharing music, make sure you are in a trusted or secure environment. To securely share music, make sure shared name is not your name or user name, and require that users use a password to access your music. When creating the password for users, use Password Assistant to help you create a strong password.

## Securing iDisk Service Access

iDisk is personal storage space for MobileMe members on Apple's Internet servers. You can use it to publish photos, websites, and movies, and to store personal data that you need access to at any time and from any computer with an Internet connection.

### iDisk Service Access

Your iDisk data is stored on Internet servers and is protected by your MobileMe account. However, if your MobileMe account is accessed by an unauthorized user, your data can be compromised. Don't store sensitive data on iDisk. Keep sensitive data local and encrypted on your computer.

### Securing Public Folder Access

When using iDisk, make sure you have a backup copy of your data. Also, when creating a MobileMe account, use a strong password. (You can use Password Assistant to help you create a strong password.)

You can protect iDisk data by creating an encrypted disk image that encrypts the data stored in it. Then you can upload this encrypted disk image to iDisk and know that your data is protected.

When sharing data on your public folder on iDisk, require users to use a password to access the data. When creating the password for your public iDisk folder, use Password Assistant to help you create a strong password.

## Securing the Back to My Mac (BTMM) Service

The new Back to My Mac (BTMM) feature in Mac OS X Leopard gives you access to other computers over the Internet. BTMM requires you to have a MobileMe account. BTMM uses your MobileMe account to create a secure connection to the computer you are accessing over the Internet. Both computers must be signed in to your MobileMe account and have BTMM enabled.

A new installation of Mac OS X Leopard has BTMM disabled by default. Also, the computer cannot be reached until sharing services are enabled in Sharing preferences. Like any other service, BTMM should remain disabled unless it is required by the system's user. Although BTMM does provide a way to set up a secure connection, this service does introduce some risks to the system, as described in this section. If BTMM is required, its use should be weighed against the security risks it may introduce.

**Note:** Using BTMM, you can only connect to computers that are running Mac OS X Leopard or later.

## BTMM Service Architecture

To provide secure connections between computers over the Internet, BTMM uses a technology called IPSec to encrypt data. To provide secure and trusted authentication, BTMM uses Kerberos with digital certificates. Kerberos eliminates the need for you to enter your username and password each time you want to reach another computer in your BTMM network.

## Securing BTMM Access

Computers in your BTMM network can discover and authenticate to configured sharing services. This introduces additional security risks to the system. Sharing services must be configured carefully to mitigate risk, as these services are designed to allow other users access to your system. Additionally, the following best practices must be completed to secure each computer in your BTMM network:

- Choose a strong password for your MobileMe account. Anyone who knows your MobileMe password can access all computers in your BTMM network. Therefore, it is important to choose a strong password and keep it safe. When creating your password, use Password Assistant to help you create a strong password.

- Consider who has physical access to your computers. Anyone who knows the login name and password of your computer can potentially access shared services on all other computers. Set a strong password for your Mac OS X user account in the Accounts pane of System Preferences.
- Before you disconnect from sharing a screen with a remote computer, lock the screen on the remote computer.

**To secure computers that are not part of your BTMM network:**

- 1 Open the Security preferences.
  - 2 Click the "Require password to wake this computer from sleep or screen saver" checkbox.
  - 3 Close Security preferences, then close System Preferences.
  - 4 Open Keychain Access (in Application/Utilities/).
  - 5 From the Keychain Access menu, choose Preferences.
  - 6 In the General pane, click the "Show Status in Menu Bar" checkbox.  
A small padlock icon appears in the menu bar. When you are away from the computer, click the padlock menu and choose Lock Screen to protect your computer.
  - 7 Disable automatic login for user accounts with a MobileMe account that is signed in.
- Performed these steps on each computer on your BTMM network.

## Securing Network Sharing Services

You can configure your computer to share files, folders, and other services with other computers on your network. You can even share your website hosted by your computer.

When sharing these services, make sure your computer has the most current Apple updates and turn off services you are not using. Also, make sure you set permissions for each service to restrict access to unauthorized users.

## DVD or CD Sharing

You can enable DVD or CD Sharing on a Mac or Windows computer to use the Remote Disc feature of MacBook Air or to share read only data stored on your DVD or CD. While your optical disc drive is shared, a user of another computer can view and access data stored on the DVD or CD in your optical disc drive.

## DVD or CD Sharing

Data transmitted between computers is not encrypted or secure, so you should only use this service in a secure environment. To prevent unauthorized users from accessing your shared optical disc drive, select the “Ask me before allowing others to use my DVD drive” checkbox to require users to request permission before they can access a DVD or CD in your Mac or Windows-based optical disc drive.

DVD or CD Sharing is turned off by default and should be off when it is not being used. This prevents unauthorized users from accessing your computer.

### From the Command Line:

```
# -----  
# Information Assurance with Services  
# -----  
# DVD or CD Sharing  
# -----  
# Disable DVD or CD Sharing.  
service com.apple.ODSAgent stop
```

## Screen Sharing (VNC)

Screen Sharing is based on virtual network computing (VNC). You can set up your computer using VNC so that others can share your screen. While your screen is shared, a user of another computer sees what’s on your screen and can open, move, and close files and windows, open applications, and even restart your computer.

### About Screen Sharing

Screen Sharing allows anyone with permission to control your computer. Data transmitted between computers is not encrypted or secure so you should only use this service in a secure environment.

Screen Sharing is turned off by default and should be off when it is not being used. This prevents unauthorized users from accessing your computer.

### Restricting Access to Specific Users

When securely configuring Screen Sharing options, grant access to only specific users to prevent unauthorized users from gaining access to your computer.

The default setting for Screen Sharing should be changed from “All users” to “Only these users.” The default setting “All users” includes all users on your local computer and all users in the directory server you are connected to. If you create a sharing user account, create a strong password using the Password Assistant.

You can also enable “VNC viewers may control screen with password” to permit VNC users to control your screen using a third-party VNC viewer with a password. The VNC password is different from the user name and password that is also required when attempting to access the computer. When creating the password, use Password Assistant to create a strong password.

#### From the Command Line:

```
# Screen Sharing (VNC)
# -----
# Disable Screen Sharing.
srm /Library/Preferences/com.apple.ScreenSharing.launchd
```

## File Sharing (AFP, FTP, and SMB)

You can set up your computer to share files and folders with other users on your network using the protocols Apple Filing Protocol (AFP), File Transfer Protocol (FTP), or Server Message Block (SMB). You can give users permission to read, write, and modify files and folders in the shared folder on your computer.

### File Sharing

When you share files and folder on your computer, you are permitting users to access the files on your computer. Permitting access requires that you maintain who has access to your files, the permissions they have, and the protocol used to access these shared files.

To securely set up File Sharing, you must configure permissions for your users. If you don't, you can create an access point for a malicious user to access your files and folders.

Depending on your environment, you can share your files using AFP, FTP, or SMB. When you share your files using AFP, user names and passwords are encrypted when the user authenticates to your computer to access files. When using SMB to share files, passwords are also encrypted when attempting to authenticate. However, SMB passwords are not securely stored on your computer.

FTP does not encrypt user names and passwords. This creates a possible way for unauthorized users to obtain the user name and password and easily access your files. Avoid using this protocol to share sensitive data. If you must use this protocol, encrypt your data using a secure encrypted image.

File Sharing is great for sharing files with others if you are in an environment where file sharing is frequent. Consider setting up a file server to prevent others from accessing your computer.

File sharing is turned off by default and should remain off when it is not being used. This prevents unauthorized users from attempting to access your computer.

## Restricting Access to Specific Users

When you configure File Sharing on your computer, you set restrictions that provide access for specific users. The users you select can be further restricted by giving them access to specific folders.

The default setting for File Sharing should be changed from “All users” to “Only these users”. The default setting “All users” includes all users on your local computer and all users in the directory server you are connected to.

You can securely configure File Sharing by restricting access to specific users. You can also restrict each user’s file permissions for each file you are sharing by using the triangles next to the user name (No Access, Read & Write, Read Only, or Write Only (Drop Box)). If you create a sharing user account, create a strong password using Password Assistant.

If you are sharing files with Windows users, you must use SMB. When you create the password for users that will use SMB, use Password Assistant to help create a strong password. The password you enter is not securely stored on the computer.

### From the Command Line:

```
# Disable File Sharing services.
# -----
# Disable FTP.
launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
# Disable SMB.
defaults delete /Library/Preferences/SystemConfiguration/ \
    com.apple.smb.server EnabledServices
launchctl unload -w /System/Library/LaunchDaemons/nmbd.plist
launchctl unload -w /System/Library/LaunchDaemons/smbd.plist
# Disable AFP.
launchctl unload -w /System/Library/LaunchDaemons/ \
    com.apple.AppleFileServer.plist
```

## Printer Sharing (CUPS)

Printer Sharing allows users on other computers to access printers connected to your computer. Make sure that this service remains disabled unless it is necessary. If it is necessary to share a printer among users, consider using dedicated print servers instead of sharing a printer from your computer. By using a dedicated print server, you won’t have printer traffic routed through your computer.



## Web Sharing (HTTP)

You can use the Apache web server software included with Mac OS X to host a website on your computer. Web sharing is off by default, and should remain disabled unless it is necessary. Some risks of Web Sharing are described below.

### Web Sharing

There are two separate websites available for users to view. Users can only view the following website located in /shortname/Sites folder if you are logged in on the computer:

http://your.computer.address/~yourusername/.

By using Web Sharing, you expose your login user name (short name). This can give hackers the ability to gain information about your computer.

The following website is located in Library/WebServer/Documents folder and is available while the Web Sharing service is running:

http://your.computer.address.

#### From the Command Line:

```
# Web Sharing
# -----
# Disable Web Sharing service.
launchctl unload -w /System/Library/LaunchDaemons/org.apache.httpd.plist
```

## Remote Login (SSH)

Remote Login allows users to connect to your computer through secure shell (SSH). By enabling Remote Login, you activate more secure versions of commonly used insecure tools.

The following table lists tools enabled with Remote Login, and their insecure counterparts.

Secure Remote Login Tool	Insecure Tool
ssh	telnet
slogin	login
scp	rcp
sftp	ftp

For more information about securing SSH, see “Enabling an SSH Connection” on page 194.

Remote Login is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

## Restricting Access to Specific Users

You can securely configure Remote Login by restricting access to specific users. The default setting for Remote Login should be changed from “All users” to “Only these users.” The default setting “All users” includes all users on your local computer and all users in the directory server you are connected to.

### From the Command Line:

```
# Remote Login (SSH)
# -----
# Disable Remote Login.
service ssh stop
```

## Enabling an SSH Connection

To set up a system as an SSH server, you must first enable Remote Login in Sharing preferences. For more information, see “Securing Sharing Preferences” on page 117.

To establish a secure SSH connection, verify that the client is receiving a valid fingerprint from the server. Fingerprints help determine the authenticity of the connection because they prove that the intended server, and not a rogue server, is receiving SSH requests from the client.

### To securely establish an SSH connection to a server for the first time:

- 1 On the server and the client, open Terminal.
- 2 On the client, enter the following command, but do not continue connecting if prompted:

```
$ ssh username@ipaddress_or_hostname
```

Replace *username* with the name of a user on the server.

Replace *ipaddress\_or\_hostname* with the IP address or host name of the server.

When you connect to a host using the IP address, entries are created in the `ssh_known_hosts` file. If you connect to the same host using its host name, a separate entry is created in the `ssh_known_host` file because each connection is treated as a unique connection.

On the server, if you select Remote Login in Sharing preferences, you are presented with a sample command showing how to connect to the server. This command includes the short name of the user you are logged in as and the IP address of the server.

- 3 On the server, enter the following command:

```
$ ssh-keygen -l -f /private/etc/ssh_host_rsa_key.pub
```

This command prints the fingerprint of the server's RSA key.

- 4 Compare the fingerprint displayed on the client with the one displayed on the server.
- 5 If they match, enter `yes` on the client.

If they do not match, your connection is not authentic.

You should never need to validate the server's fingerprint again. If you are asked to validate the server's fingerprint again, your connection has been compromised or Mac OS X has been reinstalled on the server. Verify with the server administrator to make sure that your connection is authentic.

- 6 On the client, authenticate with the server using the password for the user name you entered.
- 7 Test the connection with the server.

The name of your server should appear in the prompt.

To display your user name, enter `whoami`.

- 8 On the server and client, enter the following command:

```
$ exit
```

## Configuring a Key-Based SSH Connection

SSH supports the use of password, key, and Kerberos authentication. You can modify the `ssh` command so it only supports key-based authentication.

With key-based authentication, the client and server have public and private keys. The two computers exchange public keys. When the computers communicate with each other, they send data that is encrypted based on the other computer's public key. When a computer receives encrypted data, it can decrypt the data based on its private key.

Key-based authentication is more secure than password authentication because it requires that you have the private key file and know the password that lets you access the key file. Password authentication can be compromised without needing a private key file.

To perform this task, enable an SSH connection. For information, see "Enabling an SSH Connection" on page 194.

If the server uses FileVault to encrypt the home folder of the user you want to use SSH to connect as, you must be logged in on the server to use SSH. Alternatively, you can store the keys for the user in a location that is not protected by FileVault. However, this is not secure.

### To allow only key-based SSH connections:

- 1 On the server and the client, open Terminal.
- 2 On the server, enter the following command:

```
$ mkdir ~/.ssh
```

- 3 On the client, enter the following command:

```
$ ssh-keygen -b 1024 -t dsa
```

This command generates a public/private key pair for the client.

- 4 On the client, press Enter without entering a location when prompted for a location to store the keys.

The keys are stored in `/Users/username/.ssh/`. The public key is named `id_dsa.pub`, and the private key is named `id_dsa`.

- 5 On the client, enter a complex password when prompted for a passphrase.

A complex password is at least 12 letters long and is composed of mixed-case characters, numbers, and special characters. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 73.

- 6 On the client, enter the following command:

```
$ scp ~/.ssh/id_dsa.pub username@ipaddress_or_hostname:~/.ssh/
authorized_keys
```

Replace *username* with the name of a user on the server.

Replace *ipaddress\_or\_hostname* with the IP address or host name of the server.

This command copies the client’s public key into the server’s `~/.ssh` folder and renames the key to `authorized_keys`.

If the user needs more than one client public key on the server, then those additional public keys should be concatenated onto the end of the `authorized_keys` file. A separate key entry is required for each connection type that is used to connect to the server. For example, there is a key entry for the IP address and a key entry for the hostname of the server.

- 7 On the client, authenticate with the password of the user whose name you entered.

- 8 On the server, enter the following command and authenticate, if requested:

```
$ sudo pico /private/etc/sshd_config
```

This command loads the `sshd_config` file in the `pico` text editor. For information about how to use `pico`, enter `man pico` in a Terminal window.

- 9 On the server, edit the following lines, removing the `#` when replacing original values:

Default	Replace with	Notes
<code>#PermitRootLogin yes</code>	<code>PermitRootLogin no</code>	Prevents logging in as root through SSH. This should be set for all SSH methods of authenticating.
<code>#PasswordAuthentication yes</code>	<code>PasswordAuthentication no</code>	Disables password authentication.

Default	Replace with	Notes
#PermitEmptyPasswords no	PermitEmptyPasswords no	Denies access to accounts without passwords. This should be set for all SSH methods of authenticating.
#PubKeyAuthentication yes	PubKeyAuthentication yes	Enables key-based authentication.
#RSAAuthentication yes	RSAAuthentication no	Disables RSA authentication. (Not needed for key-based authentication.)
#RhostsRSAAuthentication no	RhostsRSAAuthentication no	Disables Rhost authentication. (Not needed for key-based authentication.)
#ChallengeResponseAuthentication yes	ChallengeResponseAuthentication no	Not needed for key-based authentication.
#UsePAM yes	UsePAM no	Not needed for key-based authentication.
#StrictModes yes	StrictModes yes	Ensures that files and folders are adequately protected by the server's permissions' scheme.
#LoginGraceTime 2m	LoginGraceTime 30	Reduces the time allowed to authenticate to 30 seconds.
#KeyRegenerationInterval 1h	KeyRegenerationInterval 3600	Ensures that the server key is changed frequently.
#ServerKeyBits 768	ServerKeyBits 1024	Requires that the server key is 1024 bits.
#Protocol 2,1	Protocol 2	Restricts OpenSSH so it uses only SSH2. This should be set for all SSH methods of authenticating.
	AllowUsers <i>username</i>	You must add this line. Replace <i>username</i> with the name of the account you want to log in as.

**10** On the client, enter the following command:

```
$ sudo pico /private/etc/sshd_config
```

**11** Authenticate, if requested.

- 12 On the client, edit the following lines:

Default	Replace with	Notes
#PasswordAuthentication yes	PasswordAuthentication no	Disables password authentication.
#RSAAuthentication yes	RSAAuthentication no	Disables RSA authentication. (Not needed for key-based authentication.)

- 13 On the client, test the SSH connection by entering the following command:

```
$ ssh username@ipaddress_or_hostname
```

Replace *username* with the name of a user on the server.

Replace *ipaddress\_or\_hostname* with the IP address or host name of the server.

When you connect to a host using the IP address, entries are created in the `ssh_known_hosts` file. If you connect to the same host using its host name, a separate entry is created in the `ssh_known_host` file because each connection is treated as a unique connection.

If successful, you are prompted to enter your passphrase for the key.

## Preventing Connection to Unauthorized Host Servers

You can prevent your computer from connecting to rogue SSH servers by modifying your `/etc/ssh_known_hosts` file. This file lists the servers you are allowed to connect to, including their domain names and their public keys.

### To prevent your computer from connecting to unauthorized servers:

- 1 If `~/.ssh/` doesn't exist, enter the following command:

```
$ mkdir ~/.ssh/
```

- 2 If `~/.ssh/known_hosts` exists, enter the following command to remove it:

```
$ srm ~/.ssh/known_hosts
```

- 3 Use SSH to connect to every server you want to allow access to by entering the following command for each server:

```
$ ssh username@ipaddress_or_hostname
```

Replace *username* with the name of a user on the server.

Replace *ipaddress\_or\_hostname* with the IP address or host name of the server.

When you connect to a host using the IP address, entries are created in the `ssh_known_hosts` file. If you connect to the same host using its host name, a separate entry is created in the `ssh_known_hosts` file because each connection is treated as a unique connection.

- 4 When you are asked to verify the server's public key fingerprint, enter `yes` if it matches the server's public key fingerprint.

You can display the server's public key fingerprint by entering the following on the server:

```
$ ssh-keygen -l -f /private/etc/ssh_host_rsa_key.pub
```

- 5 Enter the following command:

```
$ sudo cp ~/.ssh/known_hosts /etc/ssh_known_hosts
```

- 6 Authenticate, if requested.

Because `ssh_known_hosts` is located in `/etc/`, users can't modify this file unless they have administrator access.

- 7 Enter the following command:

```
$ srm ~/.ssh/known_hosts
```

After you remove `~/.ssh/known_hosts`, your computer will only connect to servers listed in `/etc/ssh_known_hosts` unless the user accepts the warning prompt.

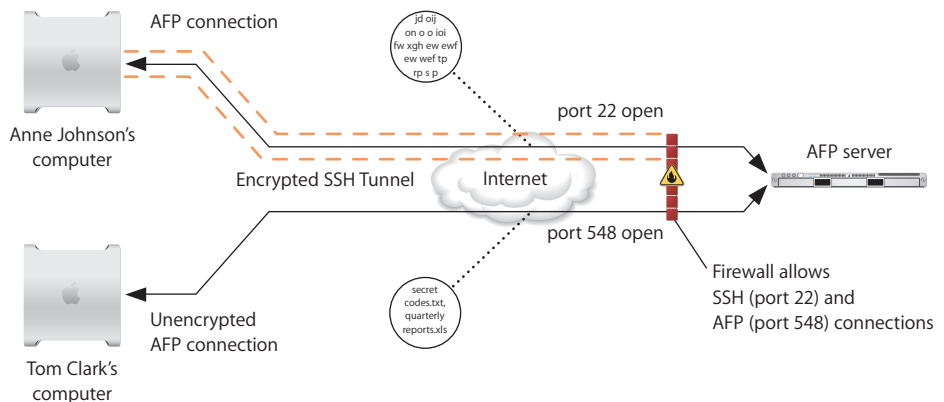
## Using SSH as a Secure Tunnel

You can use SSH to create a secure tunnel connecting to a server or client computer.

Many organizations only allow connection through a single port on the firewall to enhance network security. By using SSH tunneling, you can connect through a single port on a firewall and access a computer on the network.

This is important for computers on the network that are not configured for secure encrypted communication. SSH tunneling encrypts the data between the computer and the firewall, securing the data transmitted over an insecure network (such as the Internet).

In the following example, Anne Johnson can create an SSH tunnel that connects to an AFP server through a firewall. For additional security, this firewall should restrict all other ports. After the SSH tunnel is established, Anne Johnson can securely connect to the AFP server.



### To create an ssh tunnel:

- 1 Open Terminal.
- 2 Use the `ssh` command to create the SSH tunnel.

```
$ ssh -v -L 2501:localhost:5900 RemoteHostName -l RemoteAFPAccount
```

Replace *RemoteHostName* with the name of the host you want to connect to.

Replace *RemoteAFPAccount* with the AFP account name, and when prompted enter the password for *RemoteAFPAccount*.

- 3 Create a server in AFP.

Enter the address `localhost:2501` and the *RemoteAFPAccount* username and password.

## Modifying the SSH Configuration File

Making changes to the SSH configuration file enables you to set options for each ssh connection. You can make these changes for the system or specific users.

- To make the change for the system, change the options in the `/etc/ssh_config` file, which affects all ssh users on the computer.
- To make the change for a user, make them in the `username/.ssh/config` file.

The ssh configuration file has connection options and other specifications for a specific ssh host. A host is specified by the Host declaration. By default, the Host declaration is an asterisk ("`*`") indicating any host you are connecting to will use the options listed below the Host declaration.

You can add a specific host and options for that host by adding a new Host declaration. The new Host declaration will specify a name or address in place of the asterisk ("`*`"). You can then set the connection option for your new host below the Host declaration. This helps secure your ssh sessions in environments with different security levels.

For example, if you are connecting to a server using ssh through the Internet, the server might require a more secure or stricter connection options. However, if you are in a more secure environment, such as your own personal network, you might not need such strict connection options.

For more information about ssh configuration file options, see the `ssh` man pages.

## Generating Key Pairs for Key-Based SSH Connections

By default, SSH supports the use of password, key, and Kerberos authentication. The standard method of SSH authentication is to supply login credentials in the form of a user name and password. Key pair authentication enables you to log in to the server without supplying a password.

### This process works as follows:

- 1 A private and a public key are generated, each associated with a user name to establish that user's authenticity.



- 2 When you attempt to log in as that user, the user name is sent to the remote computer.
- 3 The remote computer looks in the user's .ssh/ folder for the user's public key.  
This folder is created after using SSH the first time.
- 4 A challenge is then sent to the user based on his or her public key.
- 5 The user verifies his or her identity by using the private portion of the key pair to decode the challenge.
- 6 After the challenge is decoded, the user is logged in without needing a password.

This is especially useful when automating remote scripts.

Key-based authentication requires possession of the private key instead of a password in order to log in to the server. A private key is much harder to guess than a password. However, if the home folder in which the private key is stored is compromised—assuming the private key is not protected by a password—then this private key could be used to log in to other systems. Password authentication can be compromised without needing a private key file.

If the server uses FileVault to encrypt the home folder of the user you want to use SSH to connect as, you must be logged in on the server to use SSH. Alternatively, you can store the keys for the user in a location that is not protected by FileVault. However, this is not secure.

#### **To generate the identity key pair:**

- 1 Enter the following command on the local computer.
- 2 When prompted, enter a filename to save the keys in the user's folder.
- 3 Enter a password followed by password verification (empty for no password).

For example:

```
Generating public/private dsa key pair.  
Enter file in which to save the key (/Users/anne/.ssh/id_dsa): frog  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in frog.  
Your public key has been saved in frog.pub.  
The key fingerprint is:  
4a:5c:6e:9f:3e:35:8b:e5:c9:5a:ac:00:e6:b8:d7:96 annejohnson1@mac.com
```

This creates two files. Your identification or private key is saved in one file (frog in our example) and your public key is saved in the other (frog.pub in our example). The key fingerprint, which is derived cryptographically from the public key value, is also displayed. This secures the public key, making it computationally infeasible for duplication.

The location of the server SSH key is `/etc/ssh_host_key.pub`. Back up your key in case you need to reinstall your server software. If your server software is reinstalled, you can retain the server identity by putting the key back in its folder.

- 4 Copy the resulting public file, which contains the local computer's public key, to the `.ssh/` folder in the user's home folder on the remote computer.

The next time you log in to the remote computer from the local computer, you won't need to enter a password (unless you entered one in step 3 above).

If you are using an Open Directory user account and you have logged in using the account, you do not need to supply a password for SSH login. On Mac OS X Server computers, SSH uses Kerberos for single sign-on authentication with any user account that has an Open Directory password (but Kerberos must be running on the Open Directory server). For more information, see the *Open Directory Administration* guide.

## Updating SSH Key Fingerprints

The first time you connect to a remote computer using SSH, the local computer prompts for permission to add the remote computer's fingerprint (or encrypted public key) to a list of known remote computers.

You might see a message like this:

```
The authenticity of host "server1.example.com" can't be established.  
RSA key fingerprint is a8:0d:27:63:74:f1:ad:bd:6a:e4:0d:a3:47:a8:f7.  
Are you sure you want to continue connecting (yes/no)?
```

The first time you connect, you have no way of knowing whether this is the correct host key. When you respond "yes," the host key is then inserted into the `~/.ssh/known_hosts` file so it can be compared against in later sessions.

Be sure this is the correct key before accepting it. If at all possible, provide your users with the encryption key through FTP, mail, or a download from the web, so they can verify the identity of the server.

If you later see a warning message about a man-in-the-middle attack when you try to connect, the key on the remote computer might no longer match the key on the local computer. This can happen if you:

- Change your SSH configuration on the local or remote computer.
- Perform a clean installation of the server software on the computer you are logging in to using SSH.
- Start up from a Mac OS X Server CD on the computer you are logging in to using SSH.
- Attempt to use SSH to log in to a computer that has the same IP address as a computer that you previously used SSH with on another network.

To connect again, delete the entries corresponding to the remote computer you are accessing (which can be stored by both name and IP address) in `~/.ssh/known_hosts`.

**Important:** Removing an entry from the `known_hosts` file bypasses a security mechanism that would help you avoid imposters and man-in-the-middle attacks. Be sure you understand why the key on the remote computer has changed before you delete its entry from the `known_hosts` file.

## Remote Management (ARD)

You can use Apple Remote Desktop (ARD) to perform remote management tasks such as screen sharing. When sharing your screen you should provide access to specific users to prevent unauthorized access to your computer screen. You also need to determine the privileges users will have when viewing your screen.

An ARD manager with full privileges can run these tasks as the root user. By limiting the privileges that an ARD manager has, you can increase security. When setting privileges, disable or limit an administrator's access to an ARD client.

You can set a VNC password that requires authorized users to use a password to access your computer. The most secure way is to require authorized users to request permission to access your computer screen.

ARD is turned off by default and should remain off when it is not being used. This prevents unauthorized users from attempting to access your computer.

## Restricting Access to Specific Users

If you need to share your screen using ARD, you must securely turn on remote management in Sharing preferences.

The default setting for remote management should be changed from "All users" to "Only these users." The default setting "All users" includes all users on your local computer and all users in the directory server you are connected to.

Any account using ARD should have limited privileges to prevent remote users from having full control of your computer.

You can securely configure ARD by restricting access to specific users. You can also restrict each user's privileges by setting ARD options. The user's privileges should be limited to the user's permission on the computer. For example, you might not want to give a standard user the ability to change your settings or delete items.

For more information, see *Apple Remote Desktop Administration Guide*.

You can also securely configure computer settings for remote management. If users connect to your computer using VNC, require that they use a password by enabling “VNC viewer may control screen with password.” Use Password Assistant to create a strong password for VNC users.

#### From the Command Line:

```
# Remote Management (ARD)
# -----
# Disable Remote Management.
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
  Resources/kickstart -deactivate -stop
```

### Remote Apple Events (RAE)

If you enable Remote Apple Events (RAE), you allow your computer to respond to events sent by other computers on your network. These events include AppleScript programs. A malicious AppleScript program can do things like delete your ~/Documents/ folder.

RAE is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

#### From the Command Line:

```
# Remote Apple Events (RAE)
# -----
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist
```

### Restricting Access to Specific Users

Avoid enabling RAE. If you enable RAE, do so on a trusted private network and disable it immediately after disconnecting from the network. The default setting for RAE should be changed from “All users” to “Only these users.” The default setting “All users” includes all users on your local computer and all users in the directory server you are connected to.

When securely configuring RAE, restrict remote events to only be accepted from specific users. This prevents unauthorized users from sending malicious events to your computer. If you create a sharing user account, create a strong password using Password Assistant. Avoid accepting events from Mac OS 9 computers. If you need to accept Mac OS 9 events, use Password Assistant to create a strong password.

## Xgrid Sharing

Computers on a network can use Xgrid to work together in a grid to process a job. Your computer can join the grid as an Xgrid client or as an Xgrid agent. A client submits jobs to the grid and an agent processes jobs received from an Xgrid controller. A controller is a server that receives jobs from clients and distributes jobs to agents.

For more information about Xgrid, see *Xgrid Administration*.

Xgrid Sharing is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

When you volunteer your computer as an agent, or when you run a grid-enabled application as a client, specify the controller by name or address. This can be done within the configuration settings of Xgrid Sharing. Also, always use a password or single sign-on for authentication.

Although your computer can use Bonjour to discover controllers on the local network, when you specify a controller, you help ensure that your computer connects to the intended Xgrid controller and not a malicious controller.

It is still possible for a malicious controller to spoof a legitimate controller's DNS and IP address, but choosing a specific controller prevents trivial attacks.

## Restricting Access to Specific Users

Your computer can specify the type of authentication it requires, including password, Kerberos, or no authentication. If your computer connects to the Internet, require some form of authentication to avoid unknowingly connecting to a malicious controller.

Malicious controllers can make agents run malicious software, create network connections, and possibly crash your computer. Similarly, clients or controllers that lack authentication might find their jobs (and sensitive data they contain) hijacked by malicious agents.

Only connect to controllers that require authentication. Password authentication is a simple authentication solution that maintains the confidentiality of your password when validating the password supplied by the controller.

After password authentication, communication with the controller is transmitted in clear text. If your connection uses Kerberos authentication, only the authentication with the controller is encrypted.

### From the Command Line:

```
# Xgrid Sharing
# -----
# Disable Xgrid Sharing.
xgridctl controller stop
xgridctl agent stop
```

## Internet Sharing

Although Internet Sharing is a convenient way to share Internet access, enabling it is a security risk. Internet Sharing also violates many organizational security policies.

Internet Sharing in Sharing preferences is preconfigured. Enabling Internet Sharing activates DHCP, NAT, and Firewall services, which are unconfigurable. A compromise to a single user node exposes the organization's network to attack.

Internet Sharing is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

### From the Command Line:

```
# Internet Sharing
# -----
# Disable Internet Sharing.
defaults write /Library/Preferences/SystemConfiguration/com.apple.nat NAT -
dict Enabled -int 0
launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.InternetSharing.plist
```

## Restricting Access to Specific Users

If you are in an environment where you need to share your Internet connection using AirPort, use the AirPort options to secure AirPort and prevent access to your computer from unauthorized users.

When configuring AirPort options to secure Internet Sharing, choose a channel from the channel pop-up menu and enable encryption using WEP.

Use a strong password for the connection, use Password Assistant to help you create a strong password, and set the WEP key length to 128 bit.

When you finish sharing your Internet connection, turn the service off.

## Bluetooth Sharing

If you have a Bluetooth module installed in your computer or if you are using an external USB Bluetooth module, you can set up your computer to use Bluetooth to send and receive files with other Bluetooth-enabled computers or devices.

You can control how your computer handles files that are exchanged between Bluetooth devices. You can choose to accept or refuse files sent to your computer and choose which folder other devices can browse.

Bluetooth Sharing is turned off by default and should remain off when it is not being used. This prevents unauthorized users from accessing your computer.

## Restricting Access to Specified Users

If you are in an environment where you would like to share files with another computer or device, use the Bluetooth Sharing options and Bluetooth preferences to securely enable Bluetooth and avoid unauthorized access to your computer.

Your Bluetooth options should always require pairing and be set to “Ask What to Do” when receiving or sharing items.

When configuring Bluetooth preferences to secure Bluetooth sharing, use the Discoverable option only while you are setting up the Bluetooth computer or device. After the device is configured, disable the Discoverable option to prevent unauthorized users from discovering your Bluetooth connection.

In the advanced section of Bluetooth preferences make sure that “Allow Bluetooth devices to wake this computer” and “Share my internet connection with other Bluetooth devices” are not selected.

### From the Command Line:

```
# Bluetooth Sharing
# -----
# Disable Bluetooth Sharing.
defaults -currentHost write com.apple.bluetooth PrefKeyServicesEnabled 0
```





Use this chapter to monitor your system and prevent attacks.

Knowing the points of your computer that are susceptible to attack can help you monitor activity and prevent attacks from occurring.

## Managing Authorization Through Rights

Authorization on Mac OS X is controlled by a policy database. This database is stored in `/etc/authorization`. The database format is described in comments at the top of that file.

The SecurityAgent plug-in processes all requests for authentication by gathering requirements from the policy database (`/etc/authorization`).

Actions can be successfully performed only when the user has acquired the rights to do so.

## Understanding the Policy Database

The policy database is a property list that consists of two dictionaries:

- The rights dictionary
- The rules dictionary

### The Rights Dictionary

The rights dictionary contains a set of key/value pairs, called *right specifications*. The key is the *right name* and the value is information about the right, including a description of what the user must do to acquire the right.

The following is an extract from the policy database installed on your system.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC ...>
<plist version="1.0">
<dict>
...
  <key>rights</key>
```

```

<dict>
  <key></key>
  <dict>
    <key>class</key>
    <string>rule</string>
    <key>comment</key>
    <string>Matches otherwise unmatched rights (i.e., is a default).</
string>
    <key>rule</key>
    <string>default</string>
  </dict>
<key>system.device.dvd.setregion.initial</key>
<dict>
  <key>class</key>
  <string>user</string>
  <key>comment</key>
  <string>Used by the DVD player to set the region code the first
time. Note that changing the region code after it has been set requires
a different right (system.device.dvd.setregion.change).</string>
  <key>group</key>
  <string>admin</string>
  <key>shared</key>
  <true/>
</dict>
...
<key>config.add.</key>
<dict>
  <key>class</key>
  <string>allow</string>
  <key>comment</key>
  <string>Wildcard right for adding rights. Anyone is allowed to add
any (non-wildcard) rights.</string>
</dict>
...

```

In this extract from the policy database, there are three rights:

- The right specification with an empty key string is known as the default right specification. To obtain this right a user must satisfy the default rule which, by default on current versions of Mac OS X, is to prove that they are an administrator.
- `system.device.dvd.setregion.initial` controls whether the user is allowed to set the initial region code for the DVD drive. By default, a user must prove that they are an administrator (in group `admin`) to set the DVD region.

- `config.add.` is a *wildcard right specification* (it ends with a dot) that matches any right whose name starts with the `config.add.` characters. This right controls whether a user can add a right specification to the policy database. By default any user can add a right specification.

When a program asks for a right, Authorization Services executes the following algorithm:

- 1 It searches the policy database for a right specification whose key exactly matches the right name.
- 2 If that fails, it searches the policy database for a wildcard right specification whose key matches the right name. If multiple right specifications are present, it uses the one with the longest key.
- 3 If that fails, it uses the default right specification.

After it has found the relevant right specification, Authorization Services evaluates the specification to decide whether to grant the right. In some cases this is easy. For example, in the extract from the policy database above, `config.add.` is always granted. In other cases it can be more complex. For example, setting the DVD region requires that you enter an administrator password.

## The Rules Dictionary

A rule consists of a set of attributes. Rules are preconfigured when Mac OS X Server is installed, but applications can change them at any time. Rules are contained in the Rules dictionary.

The following table describes the attributes defined for rules.

Rule attribute	Generic rule value	Description
key		The key is the name of a rule. A key uses the same naming conventions as a right. The Security Server uses a rule's key to match the rule with a right. Wildcard keys end with a period ("."). The generic rule has an empty key value. Rights that do not match a specific rule use the generic rule.
group	admin	The user must authenticate as a member of this group. This attribute can be set to any one group.

Rule attribute	Generic rule value	Description
shared	true	<p>If this is set to true, the Security Server marks the credentials used to gain this right as shared. The Security Server can use any shared credentials to authorize this right.</p> <p>For maximum security, set sharing to false so credentials stored by the Security Server for one application cannot be used by another application.</p>
timeout	300	<p>The credential used by this rule expires in the specified number of seconds.</p> <p>For maximum security where the user must authenticate every time, set the timeout to 0.</p> <p>For minimum security, remove the timeout attribute so the user authenticates only once per session.</p>

There are specific rules in the policy database for Mac OS X applications. There is also a generic rule in the policy database that the Security Server uses for any right that doesn't have a specific rule.

## Managing Authorization Rights

Managing authorization rights involves creating and modifying right and rule values.

### Creating an Authorization Right

To authorize a user for specific rights, you must create an authorization right in the `rights` dictionary. Each right consists of the following:

- The name of the right
- A value that contains optional data pertaining to the right
- The byte length of the value field
- Optional flags

The right always matches the generic rule unless a new rule is added to the policy database.

### Modifying an Authorization Right

To modify a right, change the value in `/etc/authorization` and save the file.

To lock out all privileged operations not explicitly allowed, change the generic rule by setting the timeout attribute to 0.

To allow all privileged operations after the user is authorized, remove the timeout attribute from the generic rule.

To prevent applications from sharing rights, set the shared attribute to false.

To require users to authenticate as a member of the staff group instead of the admin group, set the group attribute to staff.

## Example Authorization Restrictions

As an example of how the Security Server matches a right with a rule in the policy database, consider a grades-and-transcripts application.

The application requests the right `com.myOrganization.myProduct.transcripts.create`. The Security Server looks up the right in the policy database. Not finding an exact match, the Security Server looks for a rule with a wildcard key set to `com.myOrganization.myProduct.transcripts.`, `com.myOrganization.myProduct.`, `com.myOrganization.`, or `com.`—in that order—checking for the longest match.

If no wildcard key matches, the Security Server uses the generic rule.

The Security Server requests authentication from the user. The user provides a user name and password to authenticate as a member of the group admin. The Security Server creates a credential based on the user authentication and the right requested.

The credential specifies that other applications can use it, and the Security Server sets the expiration to five minutes.

Three minutes later, a child process of the application starts. The child process requests the right `com.myOrganization.myProduct.transcripts.create`.

The Security Server finds the credential, sees that it allows sharing, and uses the right. Two and a half minutes later, the same child process requests the right `com.myOrganization.myProduct.transcripts.create` again, but the right has expired.

The Security Server begins the process of creating a new credential by consulting the policy database and requesting user authentication.

## Example of Authorizing for Screen Saver

After you have configured a password-protected screen saver to prevent unauthorized users from accessing your unattended computer, modify the default rule settings of the `system.login.screensaver` (shown below) to prevent users in the admin group from being able to unlock your screen saver.

```
<key>system.login.screensaver</key>
  <dict>
    <key>class</key>
    <string>rule</string>
    <key>comment</key>
    <string>the owner as well as any admin can unlock the
screensaver;modify the group key to change this.</string>
    <key>rule</key>
    <string>authenticate-session-owner-or-admin</string>
  </dict>
  <key>system.login.tty</key>
```

The `authenticate-session-owner-or-admin` rule (shown below) permits users in the admin group or the session owner to authenticate and unlock the screen saver.

```
<key>authenticate-session-owner-or-admin</key>
  <dict>
    <key>allow-root</key>
    <false/>
    <key>class</key>
    <string>user</string>
    <key>comment</key>
    <string>the owner as well as any admin can
authorize</string>
    <key>group</key>
    <string>admin</string>
    <key>session-owner</key>
    <true/>
    <key>shared</key>
    <false/>
  </dict>
```

The default setting creates a possible point of attack, because the more users you have in the admin group the more you depend on those users to protect their user names and passwords.

The `authenticate-session-owner` rule (shown below) permits only the session owner to authenticate and unlock the screen saver.

```
<key>authenticate-session-owner</key>
  <dict>
    <key>class</key>
    <string>user</string>
    <key>comment</key>
    <string>authenticate session owner</string>
    <key>session-owner</key>
    <true/>
  </dict>
```

By changing the rule in `system.login.screensaver` (shown below) to `authenticate-session-owner`, users of the admin group cannot unlock the screen saver.

```
<key>system.login.screensaver</key>
  <dict>
    <key>class</key>
    <string>rule</string>
    <key>comment</key>
    <string>the owner as well as any admin can unlock the
screensaver;modify the group key to change this.</string>
    <key>rule</key>
    <string>authenticate-session-owner</string>
```

## Maintaining System Integrity

By monitoring events and logs you can help protect the integrity of your computer and network. Auditing and logging tools monitor your computer and help you maintain the security of your computer.

By reviewing audits and logs, you can stop login attempts from unauthorized users or computers and further protect your configuration settings.

## Validating File Integrity

When downloading files over an insecure network, the files are vulnerable to attack. Your files can be intercepted and modified by an attacker who is monitoring the insecure website activity.

For example, if you are downloading a file or program from a website that is not using SSL, your files can be intercepted and modified to become a security threat to your computer.

You can prevent this by comparing the checksum (MD5, SHA-1, or SHA-256/512 hash) value of the file you download with the original checksum value of the file, which is usually posted on the website you are downloading from.

The checksum value is a 128-bit value generated from the file you are downloading, which is like a fingerprint of the file. This value is unique to the file, and as long as the file is not modified, it always generates the same checksum value. The checksum value is generally posted on the website to use as a comparison. Only trust checksum values that are on a website that is accessed over SSL.

After you download the file, run one of the following commands on the file to generate the checksum value. The source of the file will specify which type of checksum it is:

```
$ md5 file_name
$ /usr/bin/openssl sha1 file_name
```

Then compare the checksum value you generated with the published checksum value. If the values are the same, the file has not been modified and is safe to use. If the values differ, the file has been modified or corrupted and should not be trusted. Delete the file and try downloading it again.

Mac OS X provides the checksum tools necessary for checking file validity; however, other third-party tools are available for verifying file integrity.

## About File Integrity Checking Tools

File integrity tools help protect your computer by detecting and logging changes to file system objects such as files and folders. Some file integrity tools can also detect changes to your local directory domain and to kernel modules.

Depending on the file integrity tool you choose, you can use advanced features such as the ability to reverse file system changes or to receive detailed logs in various formats.

File integrity tools are generally hosted on a server that can be securely accessed. The server retrieves logs from clients and stores baseline configuration databases and configuration data.

For more information about checksums and file hashing, see “Verifying the Integrity of Software” on page 37.

## Using Digital Signatures to Validate Applications and Processes

A digital signature uses public key cryptography to ensure the integrity of data. As with traditional signatures written with ink on paper, they can be used to identify and authenticate the signer of the data.

However, digital signatures go beyond traditional signatures because they can also ensure that the data itself has not been altered. This is like designing a check in such a way that if someone alters the amount of the sum written on the check, an “Invalid” watermark becomes visible on the face of the check.

To create a digital signature, the signer generates a message digest of the data and then uses a private key to sign the digest. The signer must have a valid digital certificate containing the public key that corresponds to the private key. The combination of a certificate and related private key is called an identity.

The signature includes the signed digest and information about the signer’s digital certificate. The certificate includes the public key and the algorithm needed to verify the signature.

To verify that the signed document has not been altered, the recipient uses the algorithm to create their own message digest and applies the public key to the signed digest. If the two digests prove identical, the message was not altered and was sent by the owner of the public key.

To ensure that the person who provided the signature is not only the same person who provided the data but is also who they say they are, the certificate is also signed—in this case by the certification authority (CA) who issued the certificate.

Signed code uses several digital signatures:



- If the code is universal, the object code for each architecture is signed separately.
- Various components of the application bundle (such as the Info.plist file, if there is one) are also signed.

## Validating Application Bundle Integrity

To validate the signature on a signed application bundle, use the `codesign` command with the `-v` option.

```
$ codesign -v code-path
```

This command verifies that the code binaries at *code-path* are signed, that the signature is valid, that all sealed components are unaltered, and that the whole bundle passes basic consistency checks. It does not by default verify that the code satisfies any requirements except its own designated requirement.

To inspect a specific requirement, use the `-R` option. For example, to verify that the Apple Mail application is identified as Mail, signed by Apple, and secured with Apple's root signing certificate, use the following command:

```
$ codesign -v -R="identifier com.apple.Mail and anchor apple"
/Applications/Mail.app
```

Unlike the `-r` option, the `-R` option takes only a single requirement rather than a requirements collection (no `=>` tags). Add additional `-v` options to get details on the validation process.

For more information about signing and verifying application bundle signatures, see the *Code Signing Guide* at [developer.apple.com/documentation/Security/Conceptual/CodeSigningGuide](https://developer.apple.com/documentation/Security/Conceptual/CodeSigningGuide). For more information about the `codesign` command, see its man page.

## Validating Running Processes

You can also use `codesign` to validate the signatures of running processes.

If you pass a number rather than a path to the verify option, `codesign` takes the number to be the process ID (pid) of a running process, and performs dynamic validation instead.

## Activity Analysis Tools

Mac OS X includes several command-line tools that you can use to analyze computer activity.

Depending on tool configurations and your computer's activity, running these tools can use a large amounts of disk space. Additionally, these tools are only effective when other users don't have administrator access. Users with administrator access can edit logs generated by the tool and circumvent the tool.

If your computer contains sensitive data, consider using auditing and logging tools. By using both types of tools, you can properly research and analyze intrusion attempts and changes in your computer's behavior.

You configure these tools to meet your organization's needs, and then change their logging settings to create relevant information for review or archiving.

## Validating System Logging

*Logging* is the recording of events, including changes to service status, processes, and operating system components. Some events are security related, while others are information messages about your computer's activity.

If an unexpected error occurs, you can analyze logs to help determine the cause of the error. For example, logs might explain why a software update can't be installed, or why you can't authenticate.

Logging tools can be useful if you have multiple users who can access the `sudo` command. You can view logs to see what users did using the `sudo` command.

Because some `sudo` commands perform additional actions that are not logged, limit the `sudo` commands that users can use. For more information, see "Securing the System Administrator Account" on page 68.

Use Console to view and maintain log files. Console is located in the /Applications/Utilities/ folder. Upon starting, the Console window shows the `console.log` file. Click Logs to display a pane that shows other log files on the system in a tree view. The tree includes folders for services such as web and mail server software.

Mac OS X log files are handled by the BSD subsystem or by a specific application. The BSD subsystem handles most important system logging, while some applications handle their own logging.

Like other BSD systems, Mac OS X uses a background process called `syslogd` to handle logging. A fundamental decision to make when configuring `syslogd` is whether to use local or remote logging. In local logging, log messages are stored on the hard disk. In remote logging, log messages are stored on a dedicated log server.

Using remote logging is strongly recommended. If computer logs are stored on a remote computer they can be analyzed; however, you must ensure the logs are transferred securely to the remote computer and that they are secure. Otherwise, the log files could be modified through a man-in-the-middle attack.

## Configuring syslogd

The configuration file for the system logging process `syslogd` is `/etc/syslog.conf`. For information about configuring this file, issue the command `man syslog.conf` in a Terminal window.

Each line of `/etc/syslog.conf` consists of text containing the following types of data.

- Facilities are categories of log messages. Standard facilities include mail, news, user, and kern (kernel).
- Priorities deal with the urgency of the message. In order from least to most critical, they are as follows: debug, info, notice, warning, err, crit, alert, and emerg. The priority of the log message is set by the application sending it, not `syslogd`.
- An action specifies what to do with the log message of a facility and priority. Messages can be sent to files, named pipes, devices, or remote hosts.

The following sample line specifies that for any log messages in the category “mail” with a priority of “emerg” or higher, the message is written to the `/var/log/mail.log` file:

```
mail.emerg /var/log/mail.log
```

The facility and priority are separated by a period, and these are separated from the action by tabs. You can use wildcards (“\*”) in the configuration file. The following sample line logs messages of any facility or priority to the file `/var/log/all.log`:

```
*.* /var/log/all.log
```

## Local System Logging

The default configuration in `/etc/newsyslog.conf` is configured for local logging in the `/var/log` folder. The computer is set to rotate log files using the periodic launchd job according to time intervals specified in the `/etc/newsyslog.conf` file.

Rotation entails compressing the current log file, incrementing the integer in the filename of compressed log files, and creating a log file for new messages.

The following table describes the rotation process after two rotations.

Files before rotation	Files after first rotation	File after second rotation
system.log	system.log	system.log
mail.log	mail.log	mail.log
	mail.log.1.gz	mail.log.1.gz
	system.log.1.gz	system.log.1.gz
		mail.log.2.gz
		system.log.2.gz

Log files are rotated by a `launchd` job, and the rotation occurs if the computer is on when the job is scheduled. By default, log rotation tasks are scheduled between midnight and 1 in the morning, to be as unobtrusive as possible to users. If the system will not be powered on at this time, adjust the settings in `/etc/newsyslog.conf`.

For information about editing the `/etc/newsyslog.conf` file, issue the `man 5 newsyslog.conf` command in a Terminal window.

## Remote System Logging

In addition to local logging, consider using remote logging. Local logs can be altered if the computer is compromised.

When deciding whether to use remote logging, consider the following issues. If these issues outweigh the benefits of remote logging, don't use remote logging.

- The `syslog` process sends log messages in the clear, which could expose sensitive information.
- Too many log messages will fill storage space on the logging system, rendering further logging impossible.
- Log files can indicate suspicious activity only if a baseline of normal activity is established and if the logs are monitored for such activity.

The following instructions assume a remote log server exists on the network.

### To enable remote logging:

- 1 Open `/etc/syslog.conf` as root.
- 2 Add the following line to the top of the file, replacing `your.log.server` with the name or IP address of the log server, and keeping all other lines intact:

```
*.* @your.log.server
```

- 3 Exit, saving changes.
- 4 Send a hangup signal to `syslogd` to make it reload the configuration file:

```
$ sudo killall -HUP syslogd
```

## Auditing System Activity

*Auditing* is the capture and maintenance of information about security-related events. Auditing helps determine the causes and the methods used for successful and failed access attempts.

Mac OS X includes a suite of auditing tools to manage, refine, and view auditing logs. You install these tools from the installation disc. For information about these auditing tools, see the *Common Criteria Configuration and Administration* guide, available at [www.apple.com/support/security/commoncriteria/](http://www.apple.com/support/security/commoncriteria/).

## Security Auditing

Auditing is the capture and maintenance of information about security-related events. Auditing helps determine the causes and methods used for successful and failed access attempts.

The audit subsystem allows authorized administrators to create, read, and delete audit information. The audit subsystem creates a log of auditable events and allows the administrator to read audit information from the records in a manner suitable for interpretation. The default location for these files is the `/var/audit/` folder.

The audit subsystem is controlled by the audit utility located in the `/usr/sbin/` folder. This utility transitions the system in and out of audit operation.

The default configuration of the audit mechanism is controlled by a set of configuration files in the `/etc/security/` folder.

If auditing is enabled, the `/etc/rc` startup script starts the audit daemon at system startup. All features of the daemon are controlled by the audit utility and the `audit_control` file.

## Installing Auditing Tools

The Common Criteria Tools disk image (.dmg) file contains the installer for auditing tools. This disk image file is available from the Common Criteria webpage located at [www.apple.com/support/security/commoncriteria/](http://www.apple.com/support/security/commoncriteria/).

After downloading the Common Criteria Tools disk image file, copy it to a removable disk, such as a CD-R disc, FireWire disk, or USB disk.

### To install the Common Criteria Tools software:

- 1 Insert the disk that contains the Common Criteria Tools disk image file and open the file to mount the volume containing the tools Installer.
- 2 Double-click the `CommonCriteriaTools.pkg` installer file.
- 3 Click Continue, then proceed through the installation by following the onscreen instructions.
- 4 When prompted to authenticate, enter the user name and password of the administrator account.

## Enabling Security Auditing

Modify the `hostconfig` file to enable auditing.

### To turn auditing on:

- 1 Open Terminal.
- 2 Enter the following command to edit the `/etc/hostconfig` file.

```
$ sudo pico /etc/hostconfig
```

- 3 Add the following entry to the file.

```
AUDIT=-YES-
```

- 4 Save the file.

Auditing is enabled when the computer starts up.

## Analyzing Security Audit Logs

If auditing is enabled, the auditing subsystem adds records of auditable events to an audit log file. The name of an audit log file consists of the date and time it was created, followed by a period, and the date and time it was terminated. For example:

```
20040322183133.20040322184443.
```

This log was created on March 22nd 2004 at 18:31:33 and was terminated on March 22nd 2004 at 18:44:43.

The audit subsystem appends records to only one audit log file at a given time. The currently active file has a suffix “.not\_terminated” instead of a date and time. Audit log files are stored in the folders specified in the audit\_control file. The audit subsystem creates an audit log file in the first folder specified.

When less than the minfree amount of disk space is available on the volume containing the audit log file, the audit subsystem:

- 1 Issues an audit\_warn soft warning
- 2 Terminates the current audit log file
- 3 Creates a new audit log file in the next specified folder

After all folders specified have exceeded this minfree limit, auditing resumes in the first folder again. However, if that folder is full, an auditing subsystem failure can occur.

You can terminate the current audit log file and create a new one manually using the audit utility. This action is commonly referred to as “rotating the audit logs.”

Use audit -n to rotate the current log file. Use audit -s to force the audit subsystem to reload its settings from the audit\_control file (which also rotates the current log file).

## Antivirus Tools

Installing antivirus tools helps prevent infection of your computer by viruses, and helps prevent your computer from becoming a host used to spread viruses to other computers. These tools quickly identify suspicious content and compare them to known malicious content.

In addition to using antivirus tools, follow computer usage habits that avoid virus infection. For example, don't download or open content you didn't request, and never open a file sent to you by someone you don't know. For more information about securely using mail, see "Mail Security" on page 157.

When you use antivirus tools, make sure you have the latest virus definition files. The protection provided by your antivirus tool depends on the quality of your virus definition files. If your antivirus program supports it, enable automatic downloading of virus definitions.

For a list of antivirus tools, see the *Macintosh Products Guide* at [guide.apple.com](http://guide.apple.com).

## Intrusion Detection Systems

An intrusion detection system (IDS) monitors user activity and examines data received through the network. You are notified of suspicious activity, and in many cases the suspicious activity is automatically prevented.

There are two types of intrusion detection systems:

- Host-based intrusion detection systems (HIDS). A HIDS monitors operating system activity on specific computers, but not network traffic. If an intruder repeats attempts to guess a login password, this can cause a HIDS alert.
- Network-based intrusion detection systems (NIDS). A NIDS examines network packets and compares them to a database of known attack patterns.

For more information, see "Intrusion Protection Using Open Source Tools" ([www.apple.com/itpro/articles/intrusionprotection/index2.html](http://www.apple.com/itpro/articles/intrusionprotection/index2.html)).





Use the checklist in this appendix to follow the steps required to secure Mac OS X.

This appendix contains checklists of action items found throughout this guide, ordered by chapter.

You can customize these checklists to suit your needs. For example, you can mark the completion status of action items in the “Completed?” column. If you deviate from the suggested action item, use the “Notes” column to justify or clarify your deviation.

Installation Action Items

For details, see Chapter 2, “Installing Mac OS X,” on page 29.

Action Item	Completed?	Notes
Securely erase the Mac OS X partition before installation		
Install Mac OS X using Mac OS Extended disk formatting		
Do not install unnecessary packages		
Do not transfer confidential information in Setup Assistant		
Do not connect to the Internet		
Create administrator accounts with difficult-to-guess names		
Create complex passwords for administrator accounts		
Do not enter a password-related hint; instead, enter help desk contact information		
Enter correct time settings		

Action Item	Completed?	Notes
Use an internal Software Update server		
Update system software using verified packages		
Repair disk permissions after installing software or software updates		

## Hardware Action Items

For details, see Chapter 3, “Protecting the System Through Hardware,” on page 41.

Action Item	Completed?	Notes
Restrict access to rooms that have computers		
Store computers in locked or secure containers when not in use		
Disable Wi-Fi Support Software		
Disable Bluetooth Support Software		
Disable Audio Recording Support Software		
Disable Video Recording Support Software		
Disable USB Support Software		
Disable FireWire Support Software		

## Global System Action Items

For details, see Chapter 4, “Securing Global System Settings,” on page 49.

Action Items	Completed?	Notes
Require an Open Firmware or EFI password		
Create an access warning for the login window		
Create an access warning for the command line		

## Account Configuration Action Items

For details, see Chapter 5, “Securing Accounts,” on page 61.

Action Item	Completed?	Notes
Create an administrator account and a standard account for each administrator		
Create a standard or managed account for each nonadministrator		
Set parental controls for managed accounts		
Restrict <code>sudo</code> users to access required commands		
Securely configure LDAPv3 access		
Securely configure Active Directory access		
Use Password Assistant to generate complex passwords		
Authenticate using a smart card, token, or biometric device		
Set a strong password policy		
Secure the login keychain		
Secure keychain items		
Create keychains for specialized purposes		
Use a portable drive to store keychains		

## System Preferences Action Items

For details, see Chapter 6, “Securing System Preferences,” on page 79.

Action Items	Completed?	Notes
Log in with administrator privileges		
Enable MobileMe only for user accounts without access to critical data		
Securely configure MobileMe preferences		
Securely configure Accounts preferences		
Securely configure Appearance preferences		
Change the number of recent items displayed		
Securely configure Bluetooth preferences		
Securely configure CD & DVD preferences		
Securely configure Date & Time preferences		
Securely configure Desktop & Screen Saver preferences		
Securely configure Display preferences		
Securely configure Dock preferences		
Securely configure Energy Saver preferences		
Configure Exposé & Spaces Preferences		
Securely configure Key & Mouse preferences		
Securely configure Network preferences		
Securely configure Parental Control preferences		
Securely configure Print & Fax preferences		
Securely configure QuickTime preferences		

Action Items	Completed?	Notes
Securely configure Security preferences		
Securely configure Sharing preferences		
Securely configure Software Update preferences		
Securely configure Sound preferences		
Securely configure Speech preferences		
Securely configure Spotlight preferences		
Securely configure Startup Disk preferences		
Securely configure Time Machine preferences		

## Encryption (DAR) Action Items

For details, see Chapter 7, “Securing Data and Using Encryption,” on page 125.

Action Items	Completed?	Notes
Assign POSIX access permissions based on user categories		
Review and modify folder flags		
Restrict Permissions on User Home Folders		
Strip setuid bits from some programs		

## Backup Action Items

For details, see Chapter 10, “Ensuring Data Integrity with Backups,” on page 147.

Action Items	Completed?	Notes
Securely encrypt and backup your data		

## Application Action Items

For details, see Chapter 11, “Information Assurance with Applications,” on page 149.

Action Items	Completed?	Notes
Configure Mail using SSL		
Verify certificate validity		
Request MobileMe identity certificate		
Secure iChat communications		
Create a strong password for iTunes		
Secure remote access using VPN		
Turn firewall protection on		

## Services Action Items

For details, see Chapter 12, “Information Assurance with Services,” on page 169.

Action Items	Completed?	Notes
Limit the list of administrators allowed to use sudo		
Disable Bonjour		
Secure BTMM access through Security Preferences		
Set up screen sharing through VNC with password protection		
Establish key-based SSH connections		
Create an SSH secure tunnel		
Configure ARD to manage remote tasks		

## Advanced Management Action Items

For details, see Chapter 13, “Advanced Security Management,” on page 209.

Action Item	Completed?	Notes
Create an authorization right to the dictionary to authorize users		
Create a digital signature		
Enable security auditing		
Configure security auditing		

Action Item	Completed?	Notes
Generate auditing reports		
Enable local logging		
Enable remote logging		
Install a file integrity checking tool		
Create a baseline configuration for file integrity checking		
Install an antivirus tool		
Configure the antivirus tool to automatically download virus definition files		





```
# Updating from an Internal Software Update Server
# -----
# Specify the software update server to use.
# Replace swupdate.apple.com with the fully qualified domain name (FQDN)
# or IP address of your software update server.
defaults write com.apple.SoftwareUpdate CatalogURL http://
    swupdate.apple.com:8088/index.sucatalog

# Switch your computer back to the default Apple update server.
defaults delete com.apple.SoftwareUpdate CatalogURL

# Updating from Internet Software Update Server
# -----
# Download and install software updates.
softwareupdate --download --all --install

# Updating Manually from Installer Packages
# -----
# Download software updates.
softwareupdate --download --all
# Install software updates.
installer -pkg $Package_Path -target /Volumes/$Target_Volume

# Verifying the Integrity of Software
# -----
# Use the sha1 command to display a file's SHA-1 digest.
# Replace $full_path_filename with the full path filename of the update
# package or image that SHA-1 digest is being checked for.
/usr/bin/openssl sha1 $full_path_filename

# Using Disk Utility to Repair Disk Permissions
# -----
# Repair disk permissions.
diskutil repairPermissions /Volumes/$Target_Boot_Drive

# -----
# Protecting the System Through Hardware
# -----
# Removing Wi-Fi Support Software
```

```

# -----
# Remove AppleAirport kernel extensions.
srms -rf /System/Library/Extensions/AppleAirPort.kext
srms -rf /System/Library/Extensions/AppleAirPort2.kext
srms -rf /System/Library/Extensions/AppleAirPortFW.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Removing Bluetooth Support Software
# -----
# Remove Bluetooth kernel extensions.
srms -rf /System/Library/Extensions/IOBluetoothFamily.kext
srms -rf /System/Library/Extensions/IOBluetoothHIDDriver.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Removing IR Support Software
# -----
# Remove IR kernel extensions.
srms -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Securing Audio Support Software
# -----
# Remove Audio Recording kernel extensions.
srms -rf /System/Library/Extensions/AppleOnboardAudio.kext
srms -rf /System/Library/Extensions/AppleUSBAudio.kext
srms -rf /System/Library/Extensions/AppleDeviceTreeUpdater.kext
srms -rf /System/Library/Extensions/IOAudioFamily.kext
srms -rf /System/Library/Extensions/VirtualAudioDriver.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Securing Video Recording Support Software
# -----
# Remove Video Recording kernel extensions.
# Remove external iSight camera.
srms -rf /System/Library/Extensions/Apple_iSight.kext
# Remove internal iSight camera.
srms -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/\
    AppleUSBVideoSupport.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Securing USB Support Software
# -----
# Remove USB kernel extensions.
srms -rf /System/Library/Extensions/IOUSBMassStorageClass.kext
# Remove Extensions cache files.

```

```

touch /System/Library/Extensions

# Securing FireWire Support Software
# -----
# Remove FireWire kernel extensions.
srm -rf /System/Library/Extensions/IOFireWireSerialBusProtocolTransport.kext
# Remove Extensions cache files.
touch /System/Library/Extensions

# Securing Global System Settings
# -----
# Configuring Open Firmware Settings
# -----
# Secure startup by setting security-mode. Replace $mode-value with
# "command" or "full".
nvram security-mode="$mode-value"
# Verify security-mode setting.
nvram -p

# Enabling Access Warning for the Login Window
# -----
# Create a login window access warning.
defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText
    "Warning Text"
# You can also used the BannerSample project to create an access warning.

# -----
# Securing System Preferences
# -----
# Securing MobileMe Preferences
# -----
# Disable Sync options.
defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer 1
# Disable iDisk Syncing.
defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool no

# Securing Accounts Preferences
# -----
# Change an account's password.
# Don't use the following command on a computer that could possibly have
# other users logged in simultaneously.
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass
# Make sure there is no password hint set.
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint -
    int 0
# Set the login options to display name and password in the login window.
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool
    yes
# Disable Show the Restart, Sleep, and ShutDown Buttons.
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
    bool yes

```

```

# Disable fast user switching.
defaults write /Library/Preferences/.GlobalPreferences
    MultipleSessionEnabled -bool NO

# Securing Appearance Preferences
# -----
# Disable display of recent applications.
defaults write com.apple.recentitems Applications -dict MaxAmount 0

# Securing Bluetooth Preferences
# -----
# Turn Bluetooth off.
defaults write /Library/Preferences/com.apple.Bluetooth \
    ControllerPowerState -int 0

# Securing CDs & DVDs Preferences
# -----
# Disable blank CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.cd.appeared -dict action 1
# Disable music CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.music.appeared -dict action 1
# Disable picture CD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.picture.appeared -dict action 1
# Disable blank DVD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.dvd.appeared -dict action 1
# Disable video DVD automatic action.
defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.dvd.video.appeared -dict action 1

# Securing Date & Time Preferences
# -----
# Set the NTP server.
cat >> /etc/ntp.conf << END server time.apple.com END
# Set the date and time.
systemsetup -settimezone $Time_Zone

# Securing Desktop & Screen Saver Preferences
# -----
# Set idle time for screen saver. XX is the idle time in seconds.
defaults -currentHost write com.apple.screensaver idleTime -int XX
# Set host corner to activate screen saver.
#wvous-bl-corner (bottom-left)
#wvous-br-corner (bottom-right)
#wvous-tl-corner (top-left)
#wvous-tr-corner (top-right)

```

```

defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-corner
    -int 5
# Set modifier key to 0 wvous-corner_code-modifier
defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
    modifier -int 0

# Securing Dock Preferences
# -----
# Automatically hide and show Dock.
defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Securing Energy Saver Preferences
# -----
# Disable computer sleep.
pmset -a sleep 0
# Enable hard disk sleep.
pmset -a disksleep 1
# Disable Wake for Ethernet network administrator access.
pmset -a womp 0
# Disable Restart automatically after power failure.
pmset -a autorestart 0

# Securing Exposé & Spaces Preferences
# -----
# Disable dashboard.
defaults write com.apple.dashboard mcx-disabled -boolean YES

# Securing Keyboard & Mouse Preferences
# -----
# Disable Bluetooth Devices to wake computer.
defaults write /Library/Preferences/com.apple.Bluetooth \
    BluetoothSystemWakeEnable -bool 0

# Securing Network Preferences
# -----
# Disable IPv6.
# The interface value can be AirPort, Bluetooth, Ethernet, or FireWire.
networksetup -setv6off $interface

# Securing Printer & Fax Preferences
# -----
# Disable the receiving of faxes.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist
# Disable printer sharing.
cp /etc/cups/cupsd.conf $TEMP_FILE
if /usr/bin/grep "Port 631" /etc/cups/cupsd.conf
then
    usr/bin/sed "/^Port 631.*s//Listen localhost:631/g" $TEMP_FILE
    > /etc/cups/cupsd.conf
else
echo "Printer Sharing not on"

```

fi

```
# Securing Security Preferences
# -----
# Enable Require password to wake this computer from sleep or screen saver.
defaults -currentHost write com.apple.screensaver askForPassword -int 1
# Disable Automatic login.
defaults write /Library/Preferences/.GlobalPreferences
com.apple.userspref.DisableAutoLogin -bool yes
# Requiring password to unlock each System Preference pane.
# Edit the /etc/authorization file using a text editor.
# Find <key>system.preferences<key>.
# Then find <key>shared<key>.
# Then replace <true/> with <false/>.
# Disable automatic login.
defaults write /Library/Preferences/.GlobalPreferences \
com.apple.autologout.AutoLogOutDelay -int 0
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
UseEncryptedSwap -bool yes
# Disable IR remote control.
defaults write /Library/Preferences/com.apple.driver.AppleIRController \
DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
/System/Library/CoreServices/ManagedClient.app/Contents/Resources/ \
createmobileaccount
# Enable Firewall.
# where value is
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
defaults write /Library/Preferences/com.apple.alf globalstate -int value
# Enable Stealth mode.
defaults write /Library/Preferences/com.apple.alf stealthenabled 1
# Enable Firewall Logging.
defaults write /Library/Preferences/com.apple.alf loggingenabled 1

# Securing Sharing Preferences
# -----
# Change computer name where $host_name is the name of the computer.
systemsetup -setcomputername $host_name
# Change computer Bonjour host name.
# The host name can not contain spaces or other non-DNS characters.
scutil --set LocalHostName $host_name

# Securing Software Updates Preferences
# -----
# Disable check for updates and Download important updates automatically.
softwareupdate --schedule off
```

```

# Securing Sound Preferences
# -----
# Disable internal microphone or line-in.
# This command does not change the input volume for all input devices, it
# only sets the default input device volume to zero.
osascript -e "set volume input volume 0"

# Securing Speech Preferences
# -----
# Disable Speech Recognition.
defaults write "com.apple.speech.recognition.AppleSpeechRecognition.prefs"
    StartSpeakableItems -bool false
# Disable Text to Speech settings.
defaults write "com.apple.speech.synthesis.general.prefs"
    TalkingAlertsSpeakTextFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
    SpokenNotificationAppActivationFlag -bool false
defaults write "com.apple.speech.synthesis.general.prefs"
    SpokenUIUseSpeakingHotKeyFlag -bool false
defaults delete "com.apple.speech.synthesis.general.prefs"
    TimeAnnouncementPrefs

# Securing Spotlight Preferences
# -----
# Disable Spotlight for a volume and erase its current meta data, where
# $volumename is the name of the volume.
$ mdutil -E -i off $volumename

# Securing Startup Disk Preferences
# -----
# Set startup disk.
systemsetup -setstartupdisk $path

# Securing Time Machine Preferences
# -----
# Enable Time Machine.
defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1

# Securing System Swap and Hibernation Storage
# -----
# Enable secure virtual memory.
defaults write /Library/Preferences/com.apple.virtualMemory \
    UseEncryptedSwap -bool YES

# -----
# Information Assurance with Services
# -----
# DVD or CD Sharing
# -----
# Disable DVD or CD Sharing.
service com.apple.ODSAgent stop

```

```

# Screen Sharing (VNC)
# -----
# Disable Screen Sharing.
srn /Library/Preferences/com.apple.ScreenSharing.launchd

# Disable File Sharing services.
# -----
# Disable FTP.
launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
# Disable SMB.
defaults delete /Library/Preferences/SystemConfiguration/ \
    com.apple.smb.server EnabledServices
launchctl unload -w /System/Library/LaunchDaemons/nmbd.plist
launchctl unload -w /System/Library/LaunchDaemons/smbd.plist
# Disable AFP.
launchctl unload -w /System/Library/LaunchDaemons/ \
    com.apple.AppleFileServer.plist

# Web Sharing
# -----
# Disable Web Sharing service.
launchctl unload -w /System/Library/LaunchDaemons/org.apache.httpd.plist

# Remote Login (SSH)
# -----
# Disable Remote Login.
service ssh stop

# Remote Management (ARD)
# -----
# Disable Remote Management.
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
    Resources/kickstart -deactivate -stop

# Remote Apple Events (RAE)
# -----
# Disable Remote Apple Events.
launchctl unload -w /System/Library/LaunchDaemons/eppc.plist

# Xgrid Sharing
# -----
# Disable Xgrid Sharing.
xgridctl controller stop
xgridctl agent stop

# Internet Sharing
# -----
# Disable Internet Sharing.
defaults write /Library/Preferences/SystemConfiguration/com.apple.nat NAT -
    dict Enabled -int 0

```



```
launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.InternetSharing.plist

# Bluetooth Sharing
# -----
# Disable Bluetooth Sharing.
defaults -currentHost write com.apple.bluetooth PrefKeyServicesEnabled 0
```



This glossary defines terms and spells out abbreviations you may encounter while working with online help or the various reference manuals for Mac OS X Server. References to terms defined elsewhere in the glossary appear in *italics*.

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

**ACE** Access Control Entry. An entry within the ACL that controls access rights. See **ACL**.

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

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

**administrator computer** A Mac OS X computer onto which you’ve installed the server administration applications from the Mac OS X Server Admin CD.

**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.

**authentication** The process of proving a user’s identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user’s level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

**authentication authority attribute** A value that identifies the password validation scheme specified for a user and provides additional information as required.

**authorization** The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an authentication process proves the user’s identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

**BIND** Berkeley Internet Name Domain. The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

**binding** A connection between a computer and a directory domain for the purpose of getting identification, authorization, and other administrative data. (verb) Also, the process of making such a connection. See also **trusted binding**.

**biometrics** A technology that authenticates a person's identity based on unique physiological or behavioral characteristics. Provides an additional factor to authentication. See **two-factor authentication**.

**blog** A webpage that presents chronologically ordered entries. Often used as an electronic journal or newsletter.

**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.

**BSD** Berkeley Software Distribution. A version of UNIX on which Mac OS X software is based.

**buffer caching** Holding data in memory so that it can be accessed more quickly than if it were repeatedly read from disk.

**cache** A portion of memory or an area on a hard disk that stores frequently accessed data in order to speed up processing times. Read cache holds data in case it's requested by a client; write cache holds data written by a client until it can be stored on disk. See also **buffer caching**, **controller cache**, **disk cache**.

**certificate** Sometimes called an "identity certificate" or "public key certificate." A file in a specific format (Mac OS X Server uses the X.509 format) that contains the public key half of a public-private keypair, the user's identity information such as name and contact information, and the digital signature of either a **Certificate Authority** (CA) or the key user.

**Certificate Authority** An authority that issues and manages digital certificates in order to ensure secure transmission of data on a public network. See also **certificate**, **public key infrastructure**.

**cluster** A collection of computers interconnected in order to improve reliability, availability, and performance. Clustered computers often run special software to coordinate the computers' activities. See also **computational cluster**.

**computational cluster** A group of computers or servers that are grouped together to share the processing of a task at a high level of performance. A computational cluster can perform larger tasks than a single computer would be able to complete, and such a grouping of computers (or “nodes”) can achieve high performance comparable to a supercomputer.

**controller** In an Xsan storage area network, short for metadata controller. In RAID systems, controller refers to hardware that manages the reading and writing of data. By segmenting and writing or reading data on multiple drives simultaneously, the RAID controller achieves fast and highly efficient storage and access. See also **metadata controller**.

**controller cache** A cache that resides within a controller and whose primary purpose is to improve disk performance.

**cracker** A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to **hacker**.

**crypt password** A type of password that’s stored as a hash (using the standard UNIX encryption algorithm) directly in a user record.

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

**decryption** The process of retrieving encrypted data using some sort of special knowledge. See also **encryption**.

**deploy** To place configured computer systems into a specific environment or make them available for use in that environment.

**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** See **folder**.

**disk cache** A cache that resides within a disk. See also **cache**, **controller cache**.

**disk image** A file that, when opened, creates an icon on a Mac OS X desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

**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.

**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."

**DoS attack** Denial of service attack. An Internet attack that uses thousands of network pings to prevent the legitimate use of a server.

**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.

**Dynamic Host Configuration Protocol** See DHCP.

**encryption** The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications. See also **decryption**.

**EFI** Extensible Firmware Interface. Software that runs automatically when an Intel-based Macintosh first starts up. It determines the computer's hardware configuration and starts the system software.

**Ethernet** A common local area networking technology in which data is transmitted in units called packets using protocols such as TCP/IP.

**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.

**firewall** Software that protects the network applications running on your server. IP firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

**firmware** Software that's stored in read-only memory (ROM) on a device and helps in starting up and operating the device. Firmware allows for certain changes to be made to a device without changing the actual hardware of the device.

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

**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.

**hacker** An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

**hash (noun)** A scrambled, or encrypted, form of a password or other text.

**host** Another name for a server.

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

**HTTP** Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. HTTP provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

**ICMP** Internet Control Message Protocol. A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round trip between two hosts to determine round-trip times and discover problems on the network.

**image** See **disk image**.

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

**installer package** A file package with the filename extension .pkg. An installer package contains resources for installing an application, including the file archive, Read Me and licensing documents, and installer scripts.

**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 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.

**IPv4** See **IP**.

**IPv6** Internet Protocol version 6. The next-generation communication protocol to replace IP (also known as IPv4). IPv6 allows a greater number of network addresses and can reduce routing loads across the Internet.

**JBoss** A full-featured Java™ application server that provides support for Java 2 Platform, Enterprise Edition (J2EE) applications.

**KDC** Kerberos Key Distribution Center. A trusted server that issues Kerberos tickets.

**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.

**kernel** The part of an operating system that handles memory management, resource allocation, and other low-level services essential to the system.

**key frame** A sample in a sequence of temporally compressed samples that doesn't rely on other samples in the sequence for any of its information. Key frames are placed into temporally compressed sequences at a frequency that's determined by the key frame rate.

**L2TP** Layer Two Tunnelling Protocol. A network transport protocol used for VPN connections. It's essentially a combination of Cisco's L2F and PPTP. L2TP itself isn't an encryption protocol, so it uses IPSec for packet encryption.

**LAN** Local area network. A network maintained within a facility, as opposed to a WAN (wide area network) that links geographically separated facilities.

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

**managed network** The items managed clients are allowed to see when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a network view.

**metadata controller** The computer that manages metadata in an Xsan storage area network.

**mutual authentication** Also known as two-way authentication. A type of authentication in which two parties authenticate with each other. For example, a client or user verifies their identity to a server, and that server confirms its identity to the client or user. Each side has the other's authenticated identity.

**NAT** Network address translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications.



**NetBoot server** A Mac OS X server you've installed NetBoot software on and have configured to allow clients to start up from disk images on the server.

**Network File System** See **NFS**.

**network view** See **managed network**.

**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.

**node** A processing location. A node can be a computer or some other device, such as a printer. Each node has a unique network address. In Xsan, a node is any computer connected to a storage area network.

**NTP** Network Time Protocol. A network protocol used to synchronize the clocks of computers across a network to some time reference clock. NTP is used to ensure that all the computers on a network are reporting the same time.

**object class** A set of rules that define similar objects in a directory domain by specifying attributes that each object must have and other attributes that each object may have.

**offline** Refers to data that isn't immediately available, or to a device that is physically connected but not available for use.

**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 Directory master** A server that provides LDAP directory service, Kerberos authentication service, and Open Directory Password Server.

**Open Directory Password Server** An authentication service that validates passwords using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

**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.

**partition** A subdivision of the capacity of a physical or logical disk. Partitions are made up of contiguous blocks on the disk.

**PDC** Primary domain controller. In Windows networking, a domain controller that has been designated as the primary authentication server for its domain.

**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**.

**phishing** An attempt to masquerade as a trusted organization or individual to trick others into divulging confidential information.

**PKI** Public Key Infrastructure. A mechanism that allows two parties to a data transaction to authenticate each other and use encryption keys and other information in identity certificates to encrypt and decrypt messages they exchange.

**POP** Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

**portable home directory** A portable home directory provides a user with both a local and network home folder. The contents of these two home folders, as well as the user's directory and authentication information, can be automatically kept in sync.

**POSIX** Portable Operating System Interface for UNIX. A family of open system standards based on UNIX, which allows applications to be written to a single target environment in which they can run unchanged on a variety of systems.

**print queue** An orderly waiting area where print jobs wait until a printer is available. The print service in Mac OS X Server uses print queues on the server to facilitate management.

**private key** One of two asymmetric keys used in a PKI security system. The private key is not distributed and is usually encrypted with a passphrase by the owner. It can digitally sign a message or certificate, claiming authenticity. It can decrypt messages encrypted with the corresponding public key and it can encrypt messages that can only be decrypted by the private key.

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

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

**proxy server** A server that sits between a client application, such as a web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

**public key** One of two asymmetric keys used in a PKI security system. The public key is distributed to other communicating parties. It can encrypt messages that can be decrypted only by the holder of the corresponding private key, and it can verify the signature on a message originating from a corresponding private key.

**public key certificate** See **certificate**.

**public key infrastructure** A secure method of exchanging data over an unsecure public network, such as the Internet, by using public key cryptography.

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

**record type** A specific category of records, such as users, computers, and mounts. For each record type, a directory domain may contain any number of records.

**recursion** The process of fully resolving domain names into IP addresses. A nonrecursive DNS query allows referrals to other DNS servers to resolve the address. In general, user applications depend on the DNS server to perform this function, but other DNS servers do not have to perform a recursive query.

**rogue computer** A computer that is set up by an attacker for the purpose of infiltrating network traffic in an effort to gain unauthorized access to your network environment.

**root** An account on a system that has no protections or restrictions. System administrators use this account to make changes to the system's configuration.

**router** A computer networking device that forwards data packets toward their destinations. A router is a special form of gateway which links related network segments. In the small office or home, the term router often means an Internet gateway, often with Network Address Translation (NAT) functions. Although generally correct, the term router more properly refers to a network device with dedicated routing hardware.

**RSA** Rivest Shamir Adleman algorithm. A public key encryption method that can be used both for encrypting messages and making digital signatures.

**SACL** Service Access Control List. Lets you specify which users and groups have access to specific services. See **ACL**.

**schema** The collection of attributes and record types or classes that provide a blueprint for the information in a directory domain.

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

**shadow password** A password that's stored in a secure file on the server and can be authenticated using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

**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.

**shared secret** A value defined at each node of an L2TP VPN connection that serves as the encryption key seed to negotiate authentication and data transport connections.

**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.

**smart card** A portable security device that contains a microprocessor. The smart card's microprocessor and its reader use a mutual identification protocol to identify each other before releasing information. The smart card is capable of securely storing passwords, certificates, and keys.

**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.

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

**SNMP** Simple Network Management Protocol. A set of standard protocols used to manage and monitor multiplatform computer network devices.

**Spotlight** A comprehensive search engine that searches across your documents, images, movies, PDF, email, calendar events, and system preferences. It can find something by its text content, filename, or information associated with it.

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

**standalone server** A server that provides services on a network but doesn't get directory services from another server or provide directory services to other computers.

**static IP address** An IP address that's assigned to a computer or device once and is never changed.

**streaming** Delivery of video or audio data over a network in real time, as a stream of packets instead of a single file download.

**subnet** A grouping on the same network of client computers that are organized by location (for example, different floors of a building) or by usage (for example, all eighth-grade students). The use of subnets simplifies administration. See also **IP subnet**.

**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.

**trusted binding** A mutually authenticated connection between a computer and a directory domain. The computer provides credentials to prove its identity, and the directory domain provides credentials to prove its authenticity.

**tunneling** A technology that allows one network protocol to send its data using the format of another protocol.

**two-factor authentication** A process that authenticates through a combination of two independent factors: something you know (such as a password), something you have (such as a smart card), or something you are (such as a biometric factor). This is more secure than authentication that uses only one factor, typically a password.

**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.

**VPN** Virtual Private Network. A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines, but they rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

**WAN** Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

**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.

**weblog** See **blog**.

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

**zone transfer** The method by which zone data is replicated among authoritative DNS servers. Slave DNS servers request zone transfers from their master servers to acquire their data.

## A

access control entries. *See* ACEs  
 access rights. *See* permissions  
 access warnings 57–60  
     *See also* permissions  
 accounts  
     administrator 32–33, 61–62, 67–70  
     authentication setup 73–85  
     checklists 227  
     creating secure 64–70  
     credential storage 77–82  
     directory domains 70–73  
     initial setup 32–33  
     mobile 70  
     nonadministrator user 61–62  
     preferences 89–91  
     security 153  
     types 61  
 ACEs (access control entries) 38, 133  
 ACLs (access control lists) 38, 78, 129, 133–134, 171–172  
 Active Directory 72–73  
 activity analysis tools 217–220  
 Address Book 71, 186  
 administrator account 32–33, 61–62, 67–70  
 Advanced Encryption Standard (AES-128) 113  
 AFP (Apple Filing Protocol) 191–192  
 antivirus tools. *See* virus screening  
 appearance preferences 92–93  
 Apple Filing Protocol. *See* AFP  
 Apple Remote Desktop. *See* ARD  
 Apple Software Restore. *See* ASR  
 Application firewall 175–177  
 applications  
     access control 24, 26, 177–178  
     securing 157–162, 216–217  
 ARD (Apple Remote Desktop) 203–204  
 ASR (Apple Software Restore) 31  
 assistive devices 128  
 attributes, rules 211  
 auditing tools 220–222  
 authentication  
     accurate time settings 33

    Active Directory 72  
     Directory Access 71–72  
     key-based SSH 200–203  
     *See also* keychain services; passwords  
     server- vs. client-side 162  
     strengthening methods 73–76  
     system preferences 86  
     user  
 authorization 209  
     *See also* authentication  
 authorization rights 212–214  
 AutoFill options 161, 166  
 automatic actions, disabling 94

## B

Back to My Mac. *See* BTMM  
 backups 155–156  
 BannerSample file, modifying 59  
 Berkeley Software Distribution. *See* BSD  
 Bill of Materials file 39  
 biometrics-based authentication 76  
 Bluetooth preferences 93–94, 207  
 Bonjour browsing service 185–187  
 bookmarks, synchronizing 165  
 Boot Camp 171–172  
 boot command 55  
 browsers  
     preferences 165  
     security 161–162  
 BSD (Berkeley Software Distribution) 20, 218  
 BTMM (Back to My Mac) 188–189

## C

CA. *See* Certificate Authority  
 cache, browser 162  
 CDs, preferences 94, 189  
 CDSA (Common Data Security Architecture) 20  
 CERT (Computer Emergency Response Team) 20  
 Certificate Assistant 162–164  
 Certificate Authority 162–164  
 Certificate Revocation List. *See* CRL  
 certificates 22, 28, 141, 157–161, 168–170  
 checksum tool 215

- CIFS (Common Internet File System). *See* SMB
- client-side authentication 162
- codesign command 217
- command-line interface
  - access warnings 59
  - erasing files 147–148
  - ssh access 193–203
  - startup security setup 56
- command-line tools, Firewall service 178
- command mode startup 55
- Common Criteria Tools 221
- Common Data Security Architecture. *See* CDSA
- Common Security Service Manager. *See* CSSM
- Computer Emergency Response Team. *See* CERT
- computers, host name 118
- configuration files 200
- Console tool 218
- contacts search policy 71–72
- cookies 162, 167
- credential storage 77–82
- CRL (Certificate Revocation List) 163
- CSSM (Common Security Service Manager) 22

## D

- Dashboard preferences 102–103
- data security 129–148, 151–152, 153, 155–156
- Date & Time preferences 95–97
- Desktop preferences 97–98
- DHCP (Dynamic Host Configuration Protocol)
  - service 173
- dictionaries
  - rights 209–211
  - rules 211
- digital signature 157–161, 216–217
- directories. *See* directory services; domains, directory; folders
- Directory Access 71–72
- directory services
  - Active Directory 72–73
  - directory domains 70–73
  - Open Directory 72
- discovery, service 71
- disk images
  - encrypting 27, 143–145, 187
  - read/write 143
  - restoring from 31
- disks
  - permissions for 37–39
  - startup 125–126
- Disk Utility 27, 38, 147, 148
- display mirroring 99
- Displays preferences 99
- Dock preferences 99
- documentation 14–16
- domains, directory 70–73

- Download Inspector 25
- DVDs, preferences 94, 189

## E

- EFI (Extensible Firmware Interface) 53, 126
- email. *See* Mail service
- encryption
  - disk images 143–146
  - FileVault 26–27, 139–143
  - Mail service 157–161
  - secure virtual memory 151–152
  - Time Machine 155–156
- Energy Saver preferences 100–101
- erasing data permanently 146–148
- Everyone permission level 130
- Exposé & Spaces preferences 102–103
- Extensible Firmware Interface. *See* EFI

## F

- fax preferences 109–111
- files
  - backup of 155–156
  - Bill of Materials 39
  - downloading safely 164–165
  - encryption 139–146
  - erasing 146–148
  - integrity checking tools 216
  - managing log 218
  - package 39
  - permissions 129–132, 134–135
  - security 151–152, 168
- file services
  - See also* FTP; share points
- file sharing 191–192
- file systems, erasing data 146
- File Transfer Protocol. *See* FTP
- FileVault 26–27, 41, 113, 139–143, 195
- FileVault master keychain 141
- fingerprints, server 194, 202–203
- Firewall service 25, 118, 174–178
- FireWire 125
- FireWire Bridge Chip GUID 125
- firmware, open password 29–30, 54–56, 125–126
- flags for files and folders 132–133
- folders
  - flags for 132–133
  - home 70, 138–143
  - permissions for 138–139
  - shared 187
- free disk space, erasing 148, 149
- FTP (File Transfer Protocol) 191–192
- full mode startup 55

## G

- global file permissions 134–135



- grids, server 205
- groups, permissions 130
- guest accounts, permissions 130
- guest operating systems 171–172

## H

- hard drive 41
- hardware, protection of 41, 226, 230
- HIDS (host-based intrusion detection systems) 223
- HiSEC (Highly Secure) templates 72
- home folders 70, 138–143
- hostconfig file 221
- host name 118
- hosts. *See* servers
- HTML (Hypertext Markup Language) email 158

## I

- iChat service 168–170, 186, 187
- iDisk 187–188
- images. *See* disk images
- installation 29–39, 119, 225–226
- installer packages 119
- Intel-based Macintosh 30, 53, 171–172
- International preferences 103
- Internet-based Software Update 34
- Internet security
  - browsers 161–162, 167
  - email 157–161
  - instant messaging 168–170
  - MobileMe preferences 87–89
  - sharing 117–118, 171, 188–189, 205–207
- intrusion detection system (IDS) monitors 223
- IP addresses 105
- IPFW2 software 178
- iPhoto 187
- IPv6 addressing 105
- iTunes 171, 187

## K

- Kerberos 72, 74–75, 157
- key-based SSH connection 195–198, 200–203
- Keyboard & Mouse preferences 103
- Keychain Access 77, 160–161, 163–164
- keychain services 22, 26, 77–82, 141

## L

- L2TP/IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) 172–173
- Launch Services 25
- layered security architecture 21
- LDAP (Lightweight Directory Access Protocol)
  - service 72, 173
- LDAPv3 access
- Lightweight Directory Access Protocol. *See* LDAP
- local system logging 219

- locking folders 132
- logging tools 218–220
- login
  - access warnings 57–60
  - automatic 112
  - keychain 78–79
  - remote 193–203, 205
  - security measures 89–91, 223

## logs

- audit 222
- Firewall service 176
- security 218–220

## M

- Mach 20
- Mail service 157–161
- managed preferences
  - Dashboard 102–103
  - Date & Time 95–97
  - Desktop 97–98
  - Displays 99
  - Dock 99
  - Energy Saver 100–101
  - Exposé & Spaces 102–103
  - International 103
  - Keyboard & Mouse 103
  - MobileMe 87–89
  - Network 105–106, 174
  - Parental Controls 106–108
  - Print & Fax 109–111
  - Security 112–115, 175
  - Sharing 117–118, 174, 194, 203–207
  - Software Update 34–37, 119
  - Sound 120
  - Spotlight 123–125
  - Startup Disk 125–126
  - Time Machine 126–127, 155–156
  - Universal Access 128
- managed user accounts 61, 153
- mandatory access controls 23–25
- Microsoft Windows compatibilities 133
- mobile accounts 70
- MobileMe preferences 87–89, 168–170

## N

- NetBoot service 31
- network-based directory domains 70–73
- network-based intrusion detection systems. *See* NIDS
- network-based keychains 82
- network install image 125
- Network preferences 174
- network services
  - access control 174
  - FileVault limitations 140, 143
  - installation 31

- keychains 82
- logs 218–220
- managed users 64
- preferences 105–106
- security methods 28, 157–178, 185–207
- sharing 117–118, 189, 205–207
- sleep mode security 100
- Software Update cautions 34
- wireless preferences 93–94
- newsyslog command 220
- NIDS (network-based intrusion detection systems) 223
- nonadministrator user accounts 61–62
- NTP (network time protocol) 33
- nvrnm tool 56

## O

- Open Directory 72
- Open Firmware interface 54
- Open Firmware password 29–30, 54–56, 125–126
- open source software 20–21
- owner permission 130

## P

- packages, file 39
- Parental Controls 25, 64–67, 106–108
- Password Assistant 73–74, 90
- passwords
  - authentication setup 73–74, 158–159
  - changing 89–91
  - command-line tools 56
  - firmware 29–30, 54–56, 125–126
  - keychain 78
  - master FileVault 140–143
  - Startup Disk preferences 125–126
  - tokens 76
  - vs. key-based authentication 195
- PDFs, encrypted 145–146
- permissions
  - access 20
  - disk 37–39
  - folders 138–139
  - manipulating 132
  - overview 129–135
  - user 192
  - viewing 130
- physical access, securing 41
- physical computers
  - hardware security 42
- PKI (public key infrastructure) 22, 157, 169, 195
  - See also* certificates
- plug-ins 167
- policy database 209–212
- portable computers
  - FileVault 139

- keychains 82
  - mobile accounts 70
- portable files, encrypting 143–146
- portable keychains 82
- POSIX (Portable Operating System Interface) 38, 130–135
- PPTP (Point-to-Point Tunneling Protocol) 173
- preferences
  - accounts 89–91
  - appearance 92–93
  - Bluetooth wireless 93–94, 207
  - CDs 94, 189
  - cookies 167
  - DVDs 94, 189
  - fax 109–111
  - overview 85–86
  - QuickTime 111–112
  - screen saver 97–98
  - See also* managed preferences
  - speech recognition 121
  - time 95–97
- Print & Fax preferences 109–111
- Printer Sharing 192
- privacy option, iChat service 169
- private browsing 162
- private key 195
- privileges vs. permissions 38
- protocols. *See specific protocols*
- proxy settings 167
- public key cryptography 216–217
- public key infrastructure. *See* PKI
- ppolicy command 76

## Q

- Quarantine 25
- QuickTime cache 111
- QuickTime preferences 111–112

## R

- read/write disk images 143
- recent items list 92–93
- Remote Apple Events 204
- remote images in email 158
- Remote Login 193–203
- remote server login 205
- remote system logging 220
- removable media
  - FileVault limitations 140, 143
- rights dictionary 209–211
- right specifications 209–211
- root permissions 53, 68–69
- rules dictionary 211

## S

- Safari preferences 161, 164–168

- sandboxing 24
- screen saver preferences 97–98, 113
- Screen Sharing 190–191
- searching preferences 123–125
- Secure Empty Trash command 148
- Secure iChat certificate 169
- secure notes 77
- Secure Sockets Layer. *See* SSL
- Secure Transport 22
- security 151–152, 153, 171
- security architecture overview 20–22
- security-mode environment variable 56
- security-password environment variable 56
- Security preferences 112–115, 175
- Server Message Block/Common Internet File System. *See* SMB
- servers
  - authentication 162–164
  - fingerprints 194, 202–203
  - securing connections 198
- server-side authentication 162
- Setup Assistant 32
- SHA-1 digest 37
- shared resources
  - printers 109, 111
  - user accounts 62
- share points 191–192
- Sharing preferences 117–118, 174, 194, 203–207
- Simple Finder 65
- single sign-on (SSO) authentication 74–75
  - See also* Kerberos
- single-user mode 53
- sleep mode, securing 100–101, 113
- smart cards 26–27, 75
- SMB (Server Message block) 191–192
- software, networking 157–178
- Software Update service 33, 34–37, 119
- Sound preferences 120
- sparse images 143
- speech recognition preferences 121
- Spotlight preferences 123–125
- `srp` command 147–148
- SSH (secure shell host) 193–203
- `ssh` command 193–203
- SSL (Secure Sockets Layer) 22, 157, 169
- standard user accounts 61
- startup, securing 53–54
- Startup Disk preferences 125–126
- stealth mode 176
- `sudo` tool 68–70
- `su` tool 68
- swap file 113
- synchronization 87–89, 165
- syslogd configuration file 219
- system administrator (root) account 68–70
- system preferences. *See* preferences

- system setup 31–33

## T

- target disk mode 126
- third-party applications 102, 112
- ticket-based authentication 72
- Time Machine 126–127, 155–156
- time settings 33, 95–97
- TLS (Transport Layer Security) protocol
- tokens, digital 76
- Transport Layer Security protocol. *See* TLS
- transport services 22
- tunneling protocols
  - SSH 199
  - VPN 172–174
- two-factor authentication 26–27

## U

- UIDs (user IDs) 62–63
- Universal Access preferences 128
- UNIX and security 20
- updating software 33–37, 119
- user accounts 61–70, 153
- user ID. *See* UID
- users
  - access control 25, 64–67, 153, 192, 212–214
  - automatic actions control 94
  - home folders 70, 138–143
  - keychain management 80–81
  - mobile 70
  - permissions 38, 130
  - preferences control 98, 102
  - root 53
  - See also* user accounts

## V

- validation, system integrity 215–216, 230
- virtual memory 113, 151–152
- Virtual Network Communication. *See* VNC
- virus screening 222
- VNC (Virtual Network Communication) 190–191
- volumes, erasing data 146
- VPN (Virtual Private Network)
  - clients 28
  - security 172–174

## W

- web browsers. *See* browsers
- web forms, completing 166
- Web Sharing 193
- websites, sharing 193
- wireless preferences 93–94

## X

- Xgrid 205

