



# Mac OS X

## Security Configuration

For Mac OS X Version 10.6 Snow Leopard

🍏 Apple Inc.  
© 2010 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  
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, Back to My Mac, Bonjour, Boot Camp, ColorSync, Exposé, FileVault, FireWire, iCal, iChat, iMac, iPhoto, iSight, iTunes, Keychain, Mac, MacBook, MacBook Air, Macintosh, Mac OS, QuickTime, Safari, Snow Leopard, Spaces, Spotlight, Tiger, Time Machine, Xgrid, Xsan, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries.

Apple Remote Desktop, Finder, and QuickTime Broadcaster are trademarks of Apple Inc.

MobileMe is a service mark of Apple Inc.

Adobe and PostScript are trademarks or registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

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.

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.

019-1828/2010-05

# Contents

## Preface

- 11 **About This Guide**
- 11 Audience
- 11 What's in This Guide
- 12 Using This Guide
- 13 Using the Command-Line Instructions from This Guide
- 13 Using Onscreen Help
  - 13 Mac Help
  - 13 Related Snow Leopard Server Security Guide
- 14 Viewing PDF Guides on Screen
- 14 Printing PDF Guides
- 14 Getting Documentation Updates
- 15 Getting Additional Information
- 16 Acknowledgments

## Chapter 1

- 17 **Introduction to Mac OS X Security Architecture**
- 18 Security Architectural Overview
  - 18 UNIX Infrastructure
  - 18 Access Permissions
  - 19 Security Framework
  - 20 Layered Security Defense
  - 20 Network Security
  - 21 Credential Management
  - 21 Public Key Infrastructure (PKI)
- 22 What's New in Snow Leopard v10.6
- 22 Existing Security Features in Snow Leopard
- 23 Signed Applications
- 23 Mandatory Access Controls
  - 24 Sandboxing
  - 24 Managed User Accounts
- 25 Enhanced Quarantining
- 26 Application-Based and IP Firewalls
- 26 Memory and Runtime Protection
- 27 Securing Sharing and Collaborative Services

27	Service Access Control Lists
27	VPN Compatibility and Integration
27	Improved Cryptography
28	Extended Validation Certificates
28	Wildcard in Identity Preferences
28	Enhanced Command-Line Tools
28	FileVault and Encrypted Storage
29	Enhanced Encrypted Disk Image Cryptography
29	Smart Card Support for Unlocking Encrypted Storage
30	Enhanced Safari 4.0 Security

## Chapter 2

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

## Chapter 3

43	<b>Securing System Hardware</b>
43	Protecting Hardware
44	Preventing Wireless Eavesdropping
45	Understanding Wireless Security Challenges
45	About OS Components
45	Removing Wi-Fi Support Software
46	Removing Bluetooth Support Software
47	Removing IR Support Software
48	Preventing Unauthorized Recording
48	Removing Audio Support Software
49	Removing Video Recording Support Software
51	Preventing Data Port Access

51	Removing USB Support Software
52	Removing FireWire Support Software
53	System Hardware Modifications
<b>Chapter 4</b>	<b>54 Securing Global System Settings</b>
54	Securing System Startup
55	Protecting Intel-Based Mac Systems
55	Using the Firmware Password Utility
56	Using Command-Line Tools for Secure Startup
57	Configuring Access Warnings
57	Enabling Access Warnings for the Login Window
58	Understanding the AuthPlugin Architecture
59	Using the BannerSample Project
60	Enabling Access Warnings for the Command Line
61	Turning On File Extensions

<b>Chapter 5</b>	<b>62 Securing System Preferences</b>
62	System Preferences Overview
64	Securing MobileMe Preferences
67	Securing Accounts Preferences
70	Securing Appearance Preferences
72	Securing Bluetooth Preferences
73	Securing CDs & DVDs Preferences
75	Securing Date & Time Preferences
77	Securing Desktop & Screen Saver Preferences
79	Securing Display Preferences
79	Securing Dock Preferences
80	Securing Energy Saver Preferences
83	Securing Exposé & Spaces Preferences
84	Securing Language & Text Preferences
84	Securing Keyboard Preferences
84	Securing Mouse Preferences
85	Securing Network Preferences
87	Network Access Control (802.1X)
88	User Profile
88	Login Window Profile
88	System Profile
89	System Profile Plus Login Window Profile
89	About Certificates in an 802.1X Environment
90	Extensible Authentication Protocol (EAP) Methods
91	Connecting to a 802.1X Network
93	Securing Managed User Accounts Preferences
96	Securing Print & Fax Preferences

99	Securing Security Preferences
99	General Security
100	FileVault Security
101	Firewall Security
104	Securing System Swap and Hibernation Storage
105	Securing Sharing Preferences
107	Securing Software Update Preferences
109	Securing Sound Preferences
110	Securing Speech Preferences
111	Securing Spotlight Preferences
114	Securing Startup Disk Preferences
115	Securing Time Machine Preferences
117	Securing Universal Access Preferences
<b>Chapter 6</b>	<b>118 Securing Accounts</b>
118	Types of User Accounts
119	Guidelines for Creating Accounts
119	Defining User IDs
120	Securing the Guest Account
121	Securing Nonadministrator Accounts
121	Controlling Local Accounts with Parental Controls
124	Securing External Accounts
124	Protecting Data on External Volumes
124	Securing Directory-Based Accounts
124	Securing Administrator Accounts
125	Securing the System Administrator Account
127	Understanding Directory Domains
128	Understanding Network Services, Authentication, and Contacts
129	Configuring LDAPv3 Access
129	Configuring Active Directory Access
130	Using Strong Authentication
130	Using Password Assistant to Generate or Analyze Passwords
131	Using Kerberos
132	Using Smart Cards
133	Using Tokens
133	Using Biometrics
134	Setting Global Password Policies
134	Storing Credentials
135	Using the Default User Keychain
136	Creating Additional Keychains
137	Securing Keychains and Their Items
138	Using Smart Cards as Keychains
139	Using Portable and Network-Based Keychains

140	About Certificates
140	Creating a Self-Signed Certificate
141	Adding Certificates to a Keychain

## Chapter 7

143	<b>Securing Data and Using Encryption</b>
143	Understanding Permissions
144	Setting POSIX Permissions
144	Viewing POSIX Permissions
145	Interpreting POSIX Permissions
146	Modifying POSIX Permissions
146	Setting File and Folder Flags
146	Viewing Flags
146	Modifying Flags
147	Setting ACL Permissions
148	Modifying ACL Permissions
148	Changing Global Umask for Stricter Default Permissions
149	Restricting Setuid Programs
152	Securing User Home Folders
153	Encrypting Home Folders
154	Overview of FileVault
154	Managing FileVault
155	Managing the FileVault Master Keychain
157	Encrypting Portable Files
157	Creating an Encrypted Disk Image
158	Creating an Encrypted Disk Image from Existing Data
159	Creating Encrypted PDFs
159	Securely Erasing Data
160	Configuring Finder to Always Securely Erase
160	Using Disk Utility to Securely Erase a Disk or Partition
161	Using Command-Line Tools to Securely Erase Files
162	Using Secure Empty Trash
162	Using Disk Utility to Securely Erase Free Space
162	Using Command-Line Tools to Securely Erase Free Space
163	Securing Guest Operating Systems with Boot Camp
163	Understanding the Time Machine Architecture
163	Deleting Permanently from Time Machine backups
164	Storing Backups Inside Secure Storage
164	Restoring Backups from Secure Storage

## Chapter 8

165	<b>Securing Applications</b>
165	Protecting Data While Using Apple Applications
165	Setting Mail Security
166	Enabling Account Security

167	Remote Content and Hidden Addresses
168	Disabling the Preview Pane for Mail Messages
169	Signing and Encrypting Mail Messages
170	Setting Web Browsing Security with Safari
171	Verifying Server Identity
172	Client-Side Authentication
172	Managing Data Communication and Execution
173	Opening Safe Files
174	Nonsecure Forms
174	Syncing Bookmarks
175	AutoFill
176	Controlling Web Content
177	Cookie Storage or Tracking Information
177	Advanced Settings
177	Securing File Downloads
178	Using Instant Message Security with iChat
179	iChat AV Security
179	Enabling Privacy
180	Enabling Encryption Using MobileMe Identity
181	Enhancing Multimedia Security with iTunes
181	Setting Photo Sharing Security with iPhoto
181	Setting Contact Sharing Security with Address Book
182	Strengthening Data Security with MobileMe
182	Securing iDisk Service Access
182	iDisk Service Access
182	Securing Public Folder Access
<b>Chapter 9</b>	<b>183 Securing Network Services</b>
183	Securing Internet Communication with Host-Based Firewalls
183	Firewall Protection
184	The Application Firewall
185	Application Firewall Architecture
185	Stealth Mode
186	Protection from Unauthorized Applications
187	The IPFW2 Firewall
187	Configuring the IPFW Firewall
187	Understanding IPFW Rulesets
188	Implementing an IPFW Ruleset
192	Protecting Data While Using Apple Services
192	Securing Remote Access Communication
192	VPN Security
194	Securing Bonjour (mDNS)
197	Securing the Back to My Mac (BTMM) Service



198	BTMM Service Architecture
198	Securing BTMM Access
199	Securing Network Sharing Services
199	DVD or CD Sharing
199	About DVD or CD Sharing
200	Screen Sharing (VNC)
200	About Screen Sharing
200	Restricting Access to Specific Users
201	File Sharing (AFP, FTP, and SMB)
201	File Sharing
202	Restricting Access to Specific Users
204	Printer Sharing (CUPS)
204	Scanner Sharing
204	Web Sharing (HTTP)
204	Web Sharing
205	Remote Login (SSH)
205	Restricting Access to Specific Users
206	Enabling an SSH Connection
207	Configuring a Key-Based SSH Connection
210	Preventing Connection to Unauthorized Host Servers
211	Using SSH as a Secure Tunnel
212	Modifying the SSH Configuration File
213	Generating Key Pairs for Key-Based SSH Connections
214	Updating SSH Key Fingerprints
215	Remote Management (ARD)
216	Restricting Access to Specific Users
216	Remote Apple Events (RAE)
217	Restricting Access to Specific Users
217	Xgrid Sharing
218	Restricting Access to Specific Users
219	Internet Sharing
219	Restricting Access to Specific Users
220	Bluetooth Sharing
220	Restricting Access to Specified Users
221	Understanding and Managing Daemons and Agents
221	Listing Active Daemons and Agents on the System
221	Configuration Files for Daemons and Agents
222	Disabling and Re-enabling Daemons and Agents
224	Where to Get Additional Information
<b>Chapter 10</b>	<b>225 Advanced Security Management</b>
	225 Managing Authorization Through Rights
	225 Understanding the Policy Database

	225	The Rights Dictionary
	227	The Rules Dictionary
	228	Managing Authorization Rights
	228	Creating an Authorization Right
	228	Modifying an Authorization Right
	229	Example Authorization Restrictions
	229	Example of Authorizing for Screen Saver
	231	Maintaining System Integrity
	231	Validating File Integrity
	232	About File Integrity Checking Tools
	232	Using Digital Signatures to Validate Applications and Processes
	233	Validating Application Bundle Integrity
	233	Validating Running Processes
	234	Using Activity Analysis Tools
	234	Validating System Logging
	235	Configuring syslogd
	235	Local System Logging
	236	Remote System Logging
	236	Auditing System Activity
	237	Security Auditing
	237	Enabling Security Auditing
	237	Analyzing Security Audit Logs
	238	Auditing Additional Events
	239	Using Antivirus Tools
	239	Using Intrusion Detection Systems
<b>Appendix A</b>	<b>240</b>	<b>Security Checklist</b>
	240	Installation Action Items
	241	Hardware Action Items
	241	Global System Action Items
	242	System Preferences Action Items
	243	Account Configuration Action Items
	244	Encryption (DAR) Action Items
	244	Application Action Items
	245	Services Action Items
	246	Advanced Management Action Items
<b>Appendix B</b>	<b>247</b>	<b>Security Scripts</b>
<b>Index</b>	<b>268</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 v10.6 Snow Leopard, and for maintaining a secure computer.

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

## Audience

This guide is for users of Mac OS X v 10.6 Snow 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 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 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 Server v10.6 Snow Leopard, 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, “Securing System 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 Snow Leopard startup. There is also information on setting up system logs to monitor system activity.
- Chapter 5, “Securing System Preferences,” describes recommended settings to secure Mac OS X system preferences.
- Chapter 6, “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 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 Applications,” describes how to protect your data while using Apple applications.
- Chapter 9, “Securing Network Services,” describes how to secure your computer services.
- Chapter 10, “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.

**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 the Command-Line Instructions from This Guide

The command-line instructions included in this document are for example only. They cannot be copied and pasted directly into a working environment and function properly.

The commands require customizing to your own environments needs and settings before they can be used. Read the appropriate man pages and usage instructions for each command before attempting to use the commands.

All the commands must be run with `sudo` or root authority. Failing to authenticate as a sudoer will result in failed commands or worse unintended consequences.

## 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.

## Related Snow Leopard Server Security Guide

If you want information about Snow Leopard Server, refer to *Mac OS X Server Security Configuration*. That guide contains information about making Snow Leopard Server and the computer it's installed on more secure, as required by enterprise and government customers.

## 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 Snow Leopard Server documentation and onscreen help is available. To view the feed use an RSS reader application, such as Safari or Mail:  
feed://helpsx.apple.com/rss/snowleopard/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/dsn/policies.html](http://www.disa.mil/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.
- *Smart Card Services Project* ([smartcardservices.macosforge.org](http://smartcardservices.macosforge.org))—The Smart Card Services Project provides instructions for implementing smart cards in Apple's Common Data Security Architecture (CDSA).

## 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 client and server security configuration guides for Mac OS X Snow Leopard.



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

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, Snow Leopard 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 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.

## Security 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 an 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 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.

## 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 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, Kerberos secures the authentication process, and a firewall prevents unauthorized access to a computer or network.
- 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.

## 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. A firewall can then filter communication over a TCP/IP connection by permitting or denying access to a computer or a network.

## 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.

## Public Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) includes certificate, key, and trust services 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.

## What's New in Snow Leopard v10.6

Mac OS X v10.6 Snow Leopard offers the following major security enhancements:

- **Increased security for memory and protection:** Snow Leopard running on the 64-bit chip improves support for memory and executable protection against arbitrary code execution. Technologies such as execute disable, library randomization, and sandboxing help prevent attacks that try to hijack or modify the software on your computer.
- **Better Trojan horse protection:** Snow Leopard maintains profiles for known malicious software, and prevents its download through many applications.
- **Increased VPN compatibility:** Virtual private network (VPN) support has been enhanced to support Cisco IPSec VPN connections without additional software.
- **Improved Cryptology technologies:** Snow Leopard includes Elliptical Curve Cryptography (ECC) support in most of its encryption technologies.
- **Support for Extended Validation Certificates:** Extended Validation (EV) Certificates requires the Certificate Authority to investigate the identity of the certificate holder before issuing a certificate.
- **Support for wildcards in domains for Keychain Access identity preferences:** This allows a client certificate-authenticated connections to multiple servers or paths defined within a single ID Pref.
- **Updated security command-line tools:** The `security` and `networksetup` command-line tools have been enhanced.
- **Enhanced Safari 4.0 security:** Safari has enhanced detection of fraudulent sites. It also runs many browser plug-ins as separate processes for enhanced security and stability.

## Existing Security Features in Snow Leopard

Snow Leopard continues to include the following security features and technologies to enhance the protection of your computer and your personal information.

- **Application signing:** This enables you to verify the integrity and identity of applications on your Mac.
- **Mandatory access control:** These enforce restrictions on access to system resources.
- **Quarantined applications:** Snow Leopard tags and marks downloaded files with first-run warnings to help prevent users from inadvertently running malicious downloaded applications.
- **Application based firewall:** After you activate the new application firewall, the firewall configures itself to restrict incoming applications without requiring the user to write complicated rules.
- **Runtime protection:** Technologies such as execute disable, library randomization, and sandboxing help prevent attacks that try to hijack or modify the software on your system.

- **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. Snow Leopard minimizes the number of security alerts that you see, so when you do see one, it gets your attention.

## Signed Applications

By signing applications, your Mac can verify the identity and integrity of an application. Applications shipped with Snow 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.

## Mandatory Access Controls

Snow Leopard uses an access control mechanism known as mandatory access controls. Although the Mandatory Access Control technology is not visible to users, it is included in Snow 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 Snow 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 Snow 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 Snow Leopard and managed preferences in Snow 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 Snow 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.

## Managed User Accounts

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. However, if an attacker has physical access to the computer ports such as USB or Firewire, Parental controls can be bypassed by mounting a disk image that contain malicious software.

You can secure these ports by disabling them. For information about disabling hardware, see Chapter 3, “Securing System Hardware.”

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 Quarantining

Applications that download files from the Internet or receive files from external sources (such as mail attachments) can use the Quarantine feature 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 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 is opened, this message does not appear again for that application and the quarantine attributes are lifted.

This mechanism dramatically reduces the number of warnings related to downloads that you see. Such messages 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.

The file and its contents are also inspected for malicious software (malware). If malware is detected, a dialog appears with the name of the malware threat contained in the file. It warns the user to move the file to the Trash or eject the image and delete the source file to prevent damage to the computer. Malware patterns are continually updated through software updates.

## Application-Based and IP Firewalls

An application-based firewall makes it easier for nonexperts to get the benefits of firewall protection. The 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, Snow Leopard signs that application to uniquely identify it. Also new in Snow Leopard, is the ability to permit all signed software to automatically receive incoming connections.

For expert users, the IPFW firewall is available. 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.

## Memory and Runtime Protection

Snow Leopard running on a 64-bit chip supports memory and executable protection. Memory and executable protection prevent specific types of malicious software from exploiting the memory allocation or execution methods to force a processor to execute arbitrary code from another process' memory area.

Snow Leopard has the following 64-bit protection features: no-execute stack, noexecute data, and no-execute heap. In Snow Leopard, no-execute stack is available for 32- and 64-bit applications. For 64-bit processes, Snow Leopard provides protection from code execution in both heap and stack data areas.

Snow Leopard also has Library Randomization. Library Randomization uses shifting memory locations for operating system processes each time the system starts up. Because an attacker cannot depend on key system processes running in known memory locations, it is very difficult to compromise the operating system.

Snow Leopard also has process sandboxing, which is a way of restricting what kinds of activities an application can perform.

## Securing Sharing and Collaborative Services

In Snow Leopard, you can configure and secure sharing services by using service access control lists (SACLs) and a secure connection.

### Service Access Control Lists

You can further secure sharing services by allowing access only to users that you specified in a service access control lists (SACLs). 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 SACLs.

### VPN Compatibility and Integration

Snow 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 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 reconfiguring 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 Snow 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 Cryptography

Snow Leopard includes Elliptical Curve Cryptography (ECC) support in most of its encryption technologies. ECC encryption is an additional mathematical model for generating and reading encryption keys. Snow Leopard supports Elliptic Curve Digital Signature Algorithm (ECDSA) for signing and key exchange.

ECC-based signatures have size and performance advantages. An ECC key of a given length can be cryptographically stronger than a DSA or RSA key of the same length. This means that a smaller ECC-based key (and therefore a faster key to process) can be just as strong as a very long RSA-based one.

ECC is supported in the following areas: TLS/SSL, S/MIME, Apple's Certificate Assistant, and Apple's `certtool` command-line tool.

## Extended Validation Certificates

Extended Validation (EV) certificates are a special type of X.509 certificate that requires the Certificate Authority (CA) to investigate the identity of the certificate holder before the CA can issue the certificate.

CAs who want to issue EV certificates must provide an investigation process that passes an independent audit, and also establishes the legal identity and legal claim to the domain name of the certificate applicant.

## Wildcard in Identity Preferences

Wildcards can now be used in domains for Keychain Access identity preferences. This allows client certificate-authenticated connections to multiple servers or paths defined within a single ID Pref.

This is often used with certificates used by Common Access Cards (CACs). For more information on Smart Cards, see “Smart Card Support for Unlocking Encrypted Storage” on page 29.

## Enhanced Command-Line Tools

The `security` command-line tool has expanded functions in Snow Leopard. Additionally, `networksetup` has been enhanced to handle importing and exporting 802.1X profiles as well as set a TLS identity on a user profile.

For more information, see the tools' respective man pages.

## FileVault and Encrypted Storage

The Disk Utility tool included in Snow Leopard enables you to create encrypted disk images, 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.

## Enhanced Encrypted Disk Image Cryptography

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 using 128-bit or even stronger 256-bit AES encryption.

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, as it is used. For example, if you open a QuickTime movie from an encrypted disk image, Snow Leopard decrypts only the portion of the movie currently playing.

## Smart Card Support for Unlocking Encrypted Storage

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

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

- Belgium National Identification Card (BELPIC)
- U.S. 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 Snow Leopard Smart Card architecture. For more information, see <http://smartcardservices.macosforge.org/>.

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.

Snow Leopard 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.

## Enhanced Safari 4.0 Security

Safari offers several kinds of enhanced security for web browsing. It supports the built-in malware scanning function, so downloaded files are checked for specific Trojan Horse attacks.

Safari also includes a fraudulent site detection feature. It works like this: Google maintains a blacklist of known and highly suspected malware-transmitting sites and phishing sites (harvesters of sensitive data). Google adds a hash of each site's URL to a database that some web browsers can use at [safebrowsing.clients.google.com](http://safebrowsing.clients.google.com).

When Safari launches, it downloads an abbreviated list of these sites' hashes. When you navigate to a web site, Safari checks the blacklist. If the website you're accessing matches a hash, Safari contacts Google for complete URL information. If it is a positive match, Safari warns you that you may be attempting to access a malware site or phishing site.

Safari stores data in the folder at `/private/var/folders/` in folders with two-letter names. The full path is `/private/var/folders/xx/yy/-Caches-/com.apple.Safari`, where "xx" and "yy" are unique codes. When you access that folder, you see Safari's cache file `Cache.db` and Google's Safe Browsing initiative blacklist file `SafeBrowsing.db`.

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 previously 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 160.

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 162.

## 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 160.

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 v10.6 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 prompted to select a disk, click Utilities > Disk Utility.
- 5 From the list of partitions, choose the partition you want to install Mac OS X on.
- 6 Click the Erase pane.
- 7 From the Format pop-up menu, choose "Mac OS Extended (Journaled)."  
Mac OS Extended disk formatting provides extended file characteristics that enhance multiplatform interoperability.
- 8 Click Erase.
- 9 When prompted with the alert "Are you sure you want to erase the partition "*name of partition*,"" click Erase.
- 10 Close Disk Utility.
- 11 Choose the partition you erased and click Customize.
- 12 From the list of packages, 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.
- 13 Click OK, then 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 *Advanced 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 40.



## 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 *System Imaging and Software Update Administration*.)

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 *System Imaging and Software Update Administration*.
- 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 In the Enter Your Apple ID screen, 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.

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."

- 4 In the Connect to Mac OS X Server screen, don't connect to a Mac OS X server.
- 5 Click Continue.

## 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 118.

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

- 1 In the Full Name and Account Name fields, enter names that are not easily guessed.  
Avoid names and account names like "administrator" and "admin."  
You can use the full or account name when you're authenticating. The account 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 130.
- 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 75.

## Turning 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.

**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 9, “Securing Network 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 38.

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, 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
# -----
# Default Settings:
# blank
# Software updates are downloaded from one of the following software update
# servers hosted by Apple:
# swscan.apple.com:80
# swquery.apple.com:80
# swcdn.apple.com:80

# Suggested Settings:
# Specify the software update server to use.
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
    CatalogURL http://swupdate.apple.com:8088/index-leopard-
    snowleopard.merged-1.sucatalog

# Available Settings:
# Replace swupdate.apple.com with the fully qualified domain name (FQDN)
# or IP address of your software update server.

# To 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 9, “Securing Network 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 40.

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 38.

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
# -----
# Default Settings:
# The softwareupdate command by default checks and lists available
# updates for download. Software Update preferences are set to the
# command-line equivalent of:
# softwareupdate --list --schedule on

# Suggested Settings:
# Download and install software updates.
sudo softwareupdate --download --all --install

# Available Settings:
# Use the following commands to view softwareupdate options:
# $ softwareupdate -h
# or
# $ man softwareupdate
```

## Updating Manually from Installer Packages

You can manually download software updates for Apple products from [support.apple.com/downloads/](http://support.apple.com/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 [support.apple.com/downloads/](http://support.apple.com/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 40.
- 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
# -----
# Default Settings:
# None

# Suggested Settings:
# Download software updates.
sudo softwareupdate --download --all
# Install software updates.
sudo installer -pkg $Package_Path -target /Volumes/$Target_Volume

# Available Settings:
# Use the following commands to view installer options:
# $ installer -h
# or
# $ man installer
```

## 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
# -----
# Default Settings:
# None

# Suggested Settings:
# 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.
sudo /usr/bin/openssl sha1 $full_path_filename

# Available Settings:
# Use the following command to view the version of OpenSSL installed on
# your computer:
# $ openssl version
# Use the following command to view openssl options:
# $ man openssl
```

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 Snow Leopard Server supports. Snow Leopard 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 144.

## 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 147.

## 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.

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. Some organizations create scripts that reapply file and folder permissions required by the organization.

#### 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 Verify Disk Permissions.

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

If permission discrepancies exist that were not set by your organization, click Repair Disk Permissions.

- 4 Choose Disk Utility > Quit Disk Utility.

#### From the command line:

```
# Using Disk Utility to Repair Disk Permissions
# -----
# Default Setting:
# None

# Suggested Setting:
# Verify disk permissions
sudo diskutil verify Permissions /Volumes/$Target_Boot_Drive
# If permission discrepancies exist that were not set by your
# organizations, use the following Repair disk permissions command:
sudo diskutil repairPermissions /Volumes/$Target_Boot_Drive

# Available Setting:
# Use the following command to view diskutil options:
# $ diskutil
```

**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 specific 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 impacts 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 guards against the content being compromised. For more information, see "Encrypting Home Folders" on page 153.

FileVault does not protect against the threat of an attacker tampering with files on the disk and reinstalling the drive. For example, an attacker could install a modified kernel, and use it to obtain your FileVault password by logging your keyboard keystrokes. To prevent such an attack, lock your computer when it is unattended. Also, if you share your computer with others, limit those who have sudoer permissions. For information about limiting sudoers, see “Securing Administrator Accounts” on page 124.

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. Whenever possible, disable wireless access 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 ensure the users’ identity, so 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 87 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 as a wireless access point 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, so turning it off might not meet your organization's wireless technology restrictions. You might need to remove components from Snow Leopard to disable them from being turned on in System Preferences.

## About 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 Snow Leopard and are also known as OS components. These kernel extensions can be removed from Snow Leopard to prevent the use of a piece of hardware.

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

**Important:** Snow Leopard 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 file to the Trash:  
IO80211Family.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 Snow Leopard.
- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

### From the command line:

```
# -----  
# Securing System Hardware  
# -----  
# Removing Wi-Fi Support Software  
# -----  
# Default setting:  
# kext files are installed and loaded.  
  
# Suggested Setting:  
# Remove Apple AirPort kernel extensions.  
sudo srm -rf /System/Library/Extensions/IO80211Family.kext  
# Remove Extensions cache files.  
sudo touch /System/Library/Extensions  
  
# Available Settings:  
# None
```

For information about turning AirPort off using `launchctl`, see “Understanding and Managing Daemons and Agents” on page 221.

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

### From the command line:

```
# Removing BlueTooth Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Bluetooth kernel extensions.
sudo srm -rf /System/Library/Extensions/IOBluetoothFamily.kext
sudo srm -rf /System/Library/Extensions/IOBluetoothHIDDriver.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## 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 by Snow Leopard.

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

From the command line:

```
# Removing IR Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove IR kernel extensions.
sudo srm -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## 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:  
AppleUSBAudio.kext  
IOAudioFamily.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 Snow Leopard.
- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

### From the command line:

```
# Securing Audio Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Audio Recording kernel extensions.
sudo srm -rf /System/Library/Extensions/AppleUSBAudio.kext
sudo srm -rf /System/Library/Extensions/IOAudioFamily.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## 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 still leaves support for external cameras.

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 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 Snow Leopard.
- 7 Choose Finder > Secure Empty Trash to delete the file.
- 8 Restart the system.

### From the command line:

```
# Securing Video Recording Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Video Recording kernel extensions.
# Remove external iSight camera.
sudo srm -rf /System/Library/Extensions/Apple_iSight.kext
# Remove internal iSight camera.
sudo srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/\
    AppleUSBVideoSupport.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## Preventing Data Port Access

Computer data ports can be easily compromised if your machine is unattended 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 55.

## 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 Snow Leopard.
- 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.
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
sudo srm -rf /System/Library/Extensions/IOUSBMassStorageClass.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## 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 Snow Leopard.

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

From the command line:

```
# Securing FireWire Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove FireWire kernel extensions.
sudo srm -rf /System/Library/Extensions/\
    IOFireWireSerialBusProtocolTransport.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
```

## 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.

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 will void your warranty.

**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). EFI is the software link between the motherboard hardware and the software operating system. EFI determine which partition or disk to load Mac OS X from. It also determines whether the user can enter single-user mode.

Single-user mode logs the user in 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 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 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 EFI Firmware password.
- Verify and set the security mode from the command line.

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

An EFI 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.

EFI 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).

## Protecting Intel-Based Mac Systems

Mac 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 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 55.

### Using the Firmware Password Utility

The Mac OS X installation disc includes the Firmware Password Utility, which you can use to enable an 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 New.
- 3 Select “Require password to start this computer from another source.”  
To disable the EFI password, deselect “Require password to start this computer from another source.” You won’t need to enter a password and verify it. Disabling the EFI password is only recommended for installing Mac OS X.
- 4 In the Password and Verify fields, enter a new EFI password and click OK.
- 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 successful.

## Using Command-Line Tools for Secure Startup

You can also configure EFI from the command line by using the `nvr` tool. However, you can only set the `security-mode` environment variable.

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 EFI.
- **Command:** This value requires a password if changes are made to EFI or if 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 EFI.

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

```
$ sudo nvr security-mode=full
```

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

From the command line:

```
# Securing Global System Settings
# -----
# Configuring EFI Settings
# -----
# Default Setting:
# security-mode is off

# Suggested Setting:
# Secure startup by setting security-mode. Replace $mode-value with
# "command" or "full."
sudo nvr security-mode="$mode-value"
# Verify security-mode setting.
sudo nvr -x -p

# Available Settings:
# security-mode:
# "command"
# "full"
# Use the following command to view the current nvr settings:
# $ nvr -x -p
# Use the following commands to view nvr options:
# $ nvr -h
# or
# $ man nvr
```



## 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:

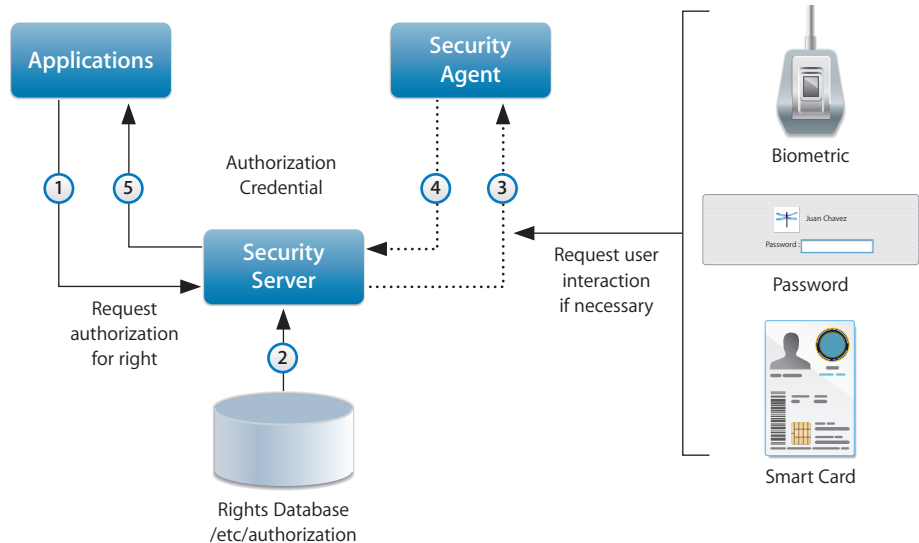
```
# Enabling Access Warning for the Login Window
# -----
# Create a login window access warning.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    LoginwindowText "Warning Text"
# You can also used the BannerSample project to create an access warning.
```

## 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 (and 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 225.

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, smart card, or biometric reader.

Then the security agent sends the authentication information back to the security server, which passes it back to the application.

## Using 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.

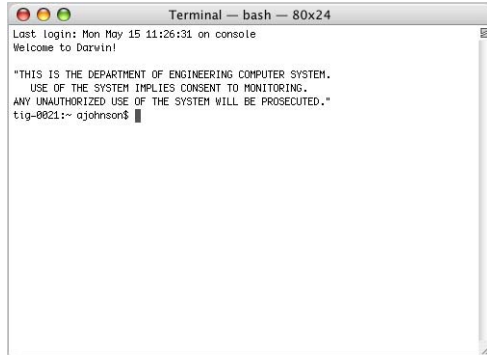
For additional information or support for the BannerSample project contact [AppleFederal@apple.com](mailto:AppleFederal@apple.com).

## 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 using 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 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.

**From the command line:**

```
# Enabling Access Warning for the Command Line
# -----
# Create a command-line access warning.
sudo touch /etc/motd
sudo chmod 644 /etc/motd
sudo echo "Warning Text" >> /etc/motd
```

## Turning On File Extensions

By making the file extension visible, you can determine the type of file it is and the application it is associated with.

**To turn file extensions on:**

- 1 Open Finder.
- 2 From the Finder menu, select Preferences.
- 3 Click Advanced and select the “Show all filename extensions” checkbox.

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 99.

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
- MobileMe
- Network
- Parental Controls
- Print & Fax
- Security
- Sharing
- Startup Disk
- Time Machine
- Universal Access

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 helps 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.

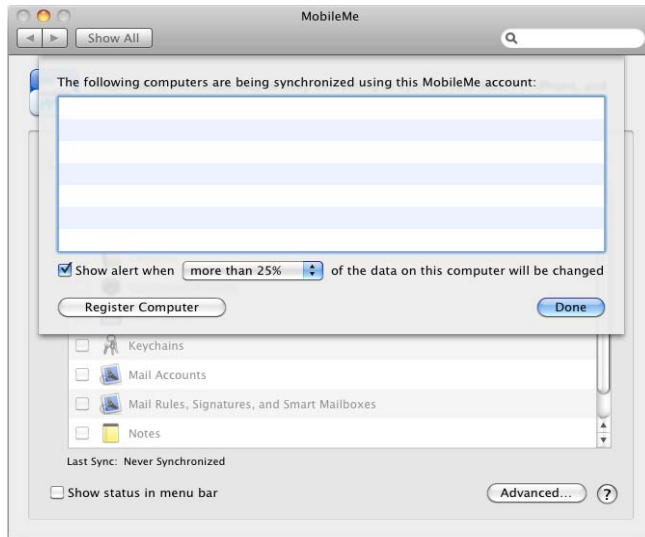
If you use MobileMe, enable it only for user accounts that don't have access to critical data. Avoid enabling MobileMe for administrator or root user accounts.

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  
# -----  
# Default Setting:  
# If a MobileMe account is entered during setup, MobileMe is configured  
# for that account.  
# Use the following command to display current MobileMe settings:  
# $ defaults -currentHost read com.apple.<Preferenceidentifier>  
# Use the following command to view all current settings for currentHost:  
# $ defaults -currentHost read  
  
# Suggested Setting:  
# Disable Sync options.  
sudo defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer  
1  
# Disable iDisk Syncing.  
sudo defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool  
no  
  
# Available Settings:  
# None
```

## 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 reset other user account passwords by selecting the account and clicking Reset Password.

**Note:** If you are an administrator, password policies are not enforced when you change your password or when you reset another user's password. Therefore, when you reset passwords as an administrator, follow the password policy that you set. For more information about password policies, see "Setting Global Password Policies" on page 134.

The password change dialog and the reset dialog (shown below) 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 more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 130.



Consider the following login guidelines:

- Modify login options to provide as little information as possible to the user.
- 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 Restart, Sleep, and Shut Down buttons—the user cannot restart the computer without pressing the power key or logging in.
- Disable fast user switching if enabled—it is a security risk because it allows multiple users to be simultaneously logged in to a computer.

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.

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 for 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.

**To securely configure Accounts preferences:**

- 1 Open Accounts preferences.
- 2 Select your 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.

To reset a user's account password, select the account and click Reset Password button. Then enter the new password and verification of the new password, and leave the password hint blank.

- 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 might have
# other users logged in simultaneously.
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass
# Make sure there is no password hint set.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    RetriesUntilHint -int 0
# Set the login options to display name and password in the login window.
sudo defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME
    -bool yes
# Disable Show the Restart, Sleep, and ShutDown Buttons.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    PowerOffDisable -bool yes
# Disable fast user switching.
sudo 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.

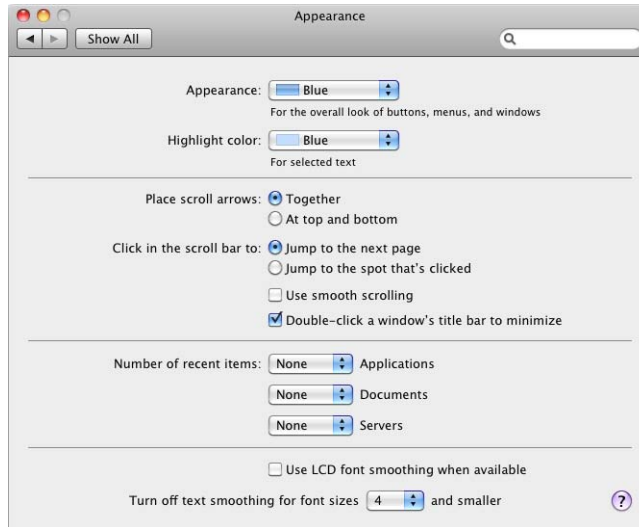
If intruders gain access to your computer, they can use recent items to quickly view your most recently accessed files. Additionally, intruders can use recent items to access authentication mechanisms for servers if the corresponding keychains are unlocked.

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
# -----
# Default Setting:
# MaxAmount 10

# Suggested Setting:
# Disable display of recent applications.
sudo defaults write com.apple.recentitems Applications -dict MaxAmount 0

# Available Settings:
# MaxAmount 0,5,10,15,20,30,50
```

## 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 118.

**To securely configure Bluetooth preferences:**

- 1 Open Bluetooth preferences.

A screen similar to the following appears:



- 2 Deselect "On."



From the command line:

```
# Securing Bluetooth Preferences
# -----
# Default Setting:
# Turn Bluetooth on.

# Suggested Setting:
# Turn Bluetooth off.
sudo defaults write /Library/Preferences/com.apple.Bluetooth\
    ControllerPowerState -int 0

# Available Settings:
# 0 (OFF) or 1 (On)
```

## 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 121.

**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
# -----
# Default Setting:
# Preference file non existent: /Library/Preferences/com.apple.digihub
# Blank CD: "Ask what to do"
# Blank DVD: "Ask what to do"
# Music CD: "Open iTunes"
# Picture CD: "Open iPhoto"
# Video DVD: "Open DVD Player"

# Suggested Setting:
# Disable blank CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.cd.appeared -dict action 1
# Disable music CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.music.appeared -dict action 1
# Disable picture CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.picture.appeared -dict action 1
# Disable blank DVD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.dvd.appeared -dict action 1
# Disable video DVD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.dvd.video.appeared -dict action 1

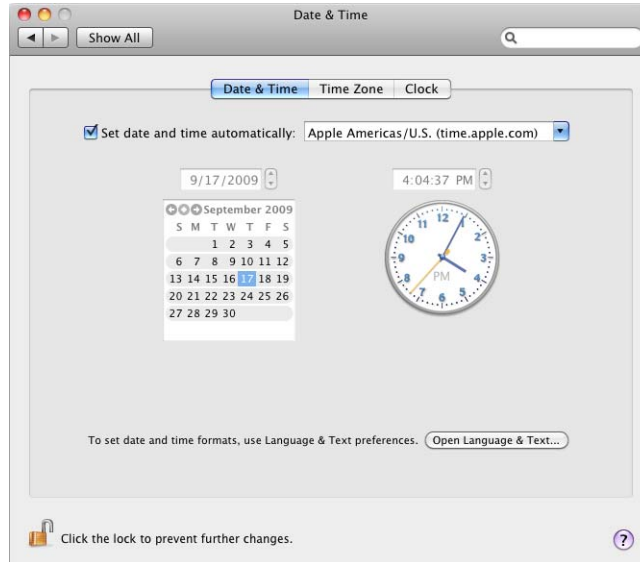
# Available Settings:
# action 1 = "Ignore"
# action 2 = "Ask what to do"
# action 5 = "Open other application"
# action 6 = "Run script"
# action 100 = "Open Finder"
# action 101 = "Open itunes"
# action 102 = "Open Disk Utility"
# action 105 = "Open DVD Player"
# action 106 = "Open iDVD"
# action 107 = "Open iPhoto"
# action 109 = "Open Front Row"
```

## 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, select the "Set data & time automatically" checkbox and enter a secure and trusted NTP server in the "Set date & time automatically" field.
- 3 Click Time Zone.

A screen similar to the following appears:



- 4 Choose a time zone from the Closest City pop-up menu.

From the command line:

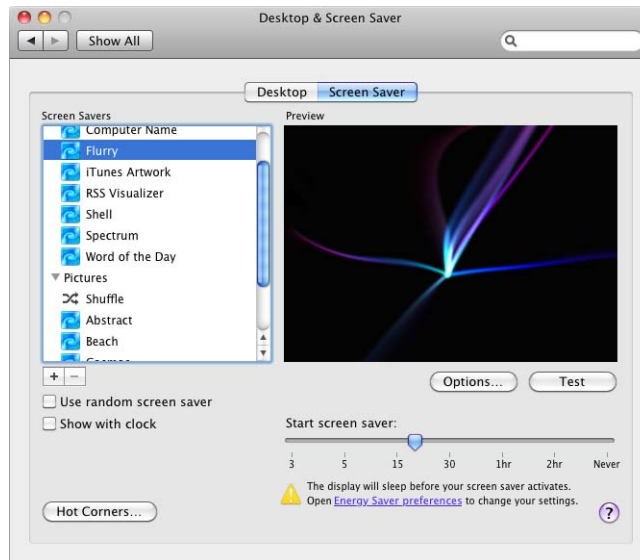
```
# Securing Date & Time Preferences
# -----
# Default Setting:
# NTP Server: time.apple.com
# Time Zone: Set time zone automatically using current location

# Suggested Setting:
# Set the NTP server.
sudo cat >> /etc/ntp.conf << END server time.apple.com END
# Set the date and time.
sudo systemsetup -settimezone $Time_Zone

# Available Settings:
# NTP Server: Any valid NTP server
# Time Zone: /usr/share/zoneinfo
```

## Securing Desktop & Screen Saver Preferences

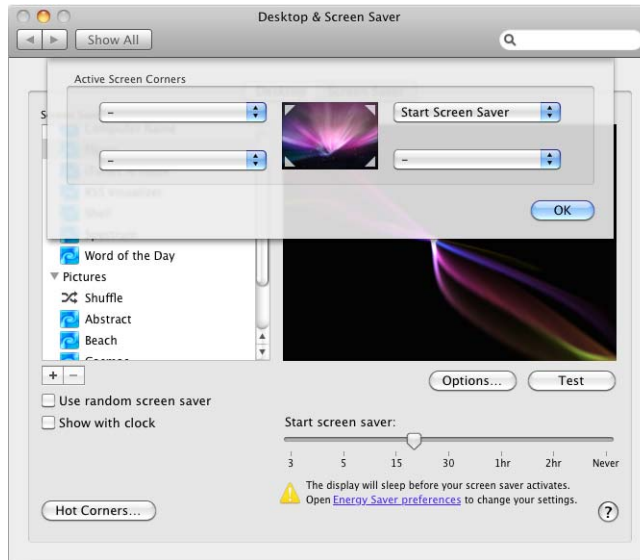
You can use Desktop & Screen Saver preferences (shown below) to configure a password-protected screen saver to prevent unauthorized users from accessing unattended computers.



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 99.

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 118.

**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
# -----
# Default Setting:
# None

# Suggested Setting:
# Set idle time for screen saver. Replace XX with the idle time in seconds.
sudo defaults -currentHost write com.apple.screensaver idleTime -int XX
# Set host corner to activate screen saver.
sudo defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
corner -int 5
# Set modifier key to 0 wvous-corner_code-modifier
sudo defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
modifier -int 0

# Available Settings:
# Corner options:
# wvous-bl-corner (bottom-left)
# wvous-br-corner (bottom-right)
# wvous-tl-corner (top-left)
# wvous-tr-corner (top-right)
```

## 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.

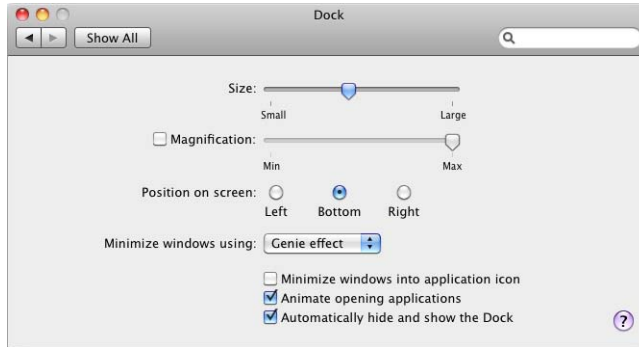
## Securing Dock Preferences

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
# -----
# Default Setting:
# None

# Suggested Setting:
# Automatically hide and show Dock.
sudo defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Available Settings:
# autohide -bool YES
# autohide -bool NO
```

## 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 99). This is similar to using a password-protected screen saver.

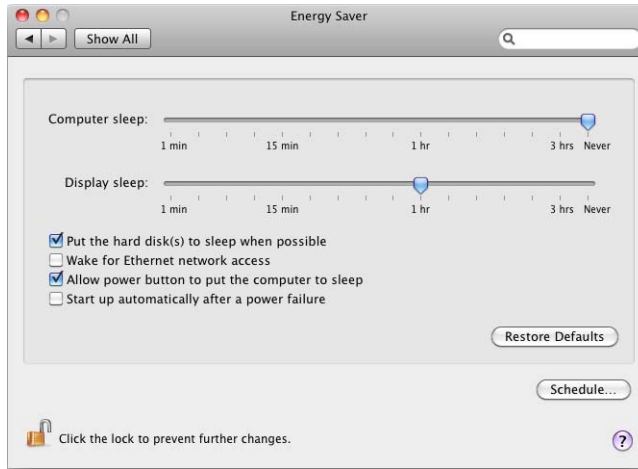


You can also use the Options pane to make settings depending on your power supply (power adapter, UPS, or battery). Configure the computer so it only wakes when you physically access the computer. Also, don't set the computer to restart after a power failure.

**To securely configure Energy Saver preferences:**

- 1 Open Energy Saver preferences.

A screen similar to the following appears:



- 2 Set "Computer sleep" to Never.
- 3 Select "Put the hard disk(s) to sleep when possible" and then click the "Options" pane.
- 4 Deselect "Wake for Ethernet network access" and "Startup automatically after a power failure."

From the command line:

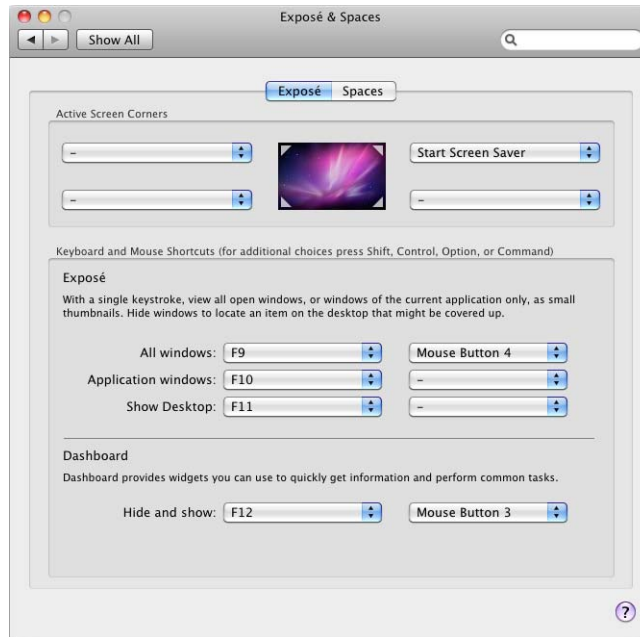
```
# Securing Energy Saver Preferences
# -----
# Default Setting:
# None

# Suggested Setting:
# Disable computer sleep.
sudo pmset -a sleep 0
# Enable hard disk sleep.
sudo pmset -a disksleep 1
# Disable Wake for Ethernet network administrator access.
sudo pmset -a womp 0
# Disable Restart automatically after power failure.
sudo pmset -a autorestart 0

# Available Settings:
# 0 (OFF) or 1 (ON)
```

## 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 99.

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 118.

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
# -----
# Default Setting:
# Enabled

# Suggested Setting:
# Disable dashboard.
sudo launchctl unload -w /System/Library/LaunchDaemons/
    com.apple.dashboard.advisory.fetch.plist

# Available Settings:
# Enabled or Disabled
```

## Securing Language & Text 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 Preferences

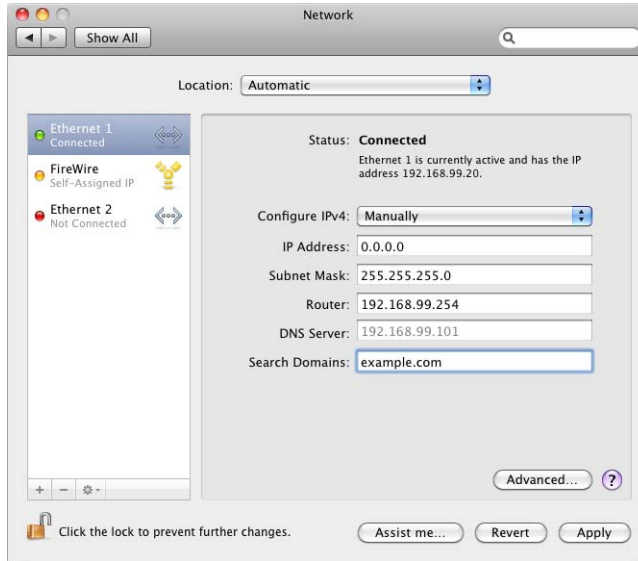
If you are not using a Bluetooth keyboard, turn Bluetooth off. If you are using a Bluetooth keyboard, disable allowing Bluetooth devices to awake the computer in the advanced section of Bluetooth preferences. For more information about Bluetooth, see “Bluetooth Sharing” on page 220.

## Securing Mouse Preferences

If you are not using a Bluetooth mouse, turn Bluetooth off. If you are using a Bluetooth mouse, disable allowing Bluetooth devices to awake the computer in the advanced section of Bluetooth preferences. For more information about Bluetooth, see “Bluetooth Sharing” on page 220.

## 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.

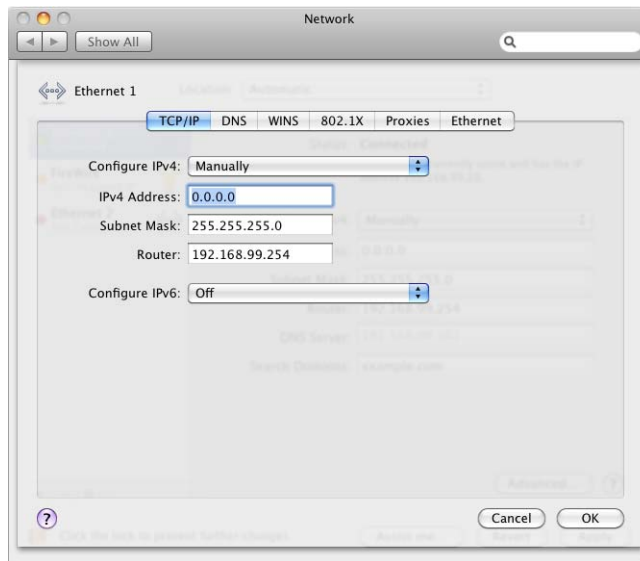
By default IPv6 is configured automatically, and the default settings are sufficient for most computers that use IPv6. You can also configure IPv6 manually. If your organization's network cannot use or does not require IPv6, turn it off.

### To securely configure Network preferences:

- 1 Open Network preferences.
- 2 From the list of hardware devices, select the hardware device you don't use (for example, AirPort, Ethernet, or FireWire).

- 3 Click the Action button below the list of hardware devices and select “Make Service Inactive”.
- 4 Repeat steps 2 and 3 to deactivate the devices that you don’t use.
- 5 From the list of hardware devices, select the hardware device you use to connect to your network (for example, Airport or Ethernet).
- 6 From the Configure IPv4 pop-up menu, choose Manually.  
Enter your static IP address, Subnet Mask, Router, DNS Server, and Search Domain configuration settings.
- 7 Click Advanced.

A screen similar to the following appears:



- 8 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.
- 9 Click OK.

From the command line:

```
# Securing Network Preferences
# -----
# Default Setting:
# Enabled

# Suggested Setting:
# Disable IPv6.
sudo networksetup -setv6off $interface

# Available Settings:
# The interface value can be AirPort, Bluetooth, Ethernet, or FireWire.
```

## 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.

The 802.1X standard enhances the security of LANs by preventing unauthorized devices from gaining access to the network through wired or wireless LAN connections. It supports a wide range of authentication methods, including TLS, EAP-FAST, TTLS, LEAP, MD5, and PEAP.

You might need to connect to a wireless (IEEE 802.11) or Ethernet (IEEE 802.3) network that is protected by the 802.1X standard if you are in an education or business environment. In an 802.1X secured environment, a computer cannot gain access to network services, such as email or the Internet, until it is authenticated.

When configuring your 802.1X settings in Snow Leopard, you'll need one or all of the following information depending on the security method being used:

- User name and password
- Wireless network name (case sensitive)
- Authentication methods and options
- Server certificate or certificate chain

If you are using TLS, you need a user or machine identity (certificate or private key), commonly distributed in a .p12 file (PKCS12).

Snow Leopard uses a concept of profiles to implement the 802.1X standard. The authentication server does not understand the concept of profiles, nor does it care. Authentication through any of the profile types is standards-based.

## User Profile

A User profile is the most basic profile type. Because an 802.1X session runs as the user during user mode, the authentication session starts after the user is logged into the computer.

A User profile cannot be used if the computer is bound to a directory server such as Open Directory and requires directory authentication to log into the computer. For computers bound to a directory server, a System profile or a Login Window profile is required.

## Login Window Profile

In the Login Window mode the 802.1X session originates from the login window using credentials entered at the login window. The same credentials are used to authenticate to the network and to authenticate the user to a directory service.

At the login screen, a user enters a user name and password. If Login Window can't find a local user account with that name, it initiates an 802.1X session using the same name and password. In the case of an 802.11 network it also associates to the wireless network. After the 802.1X authentication completes, Login Window authenticates the user with the directory service. If that authentication succeeds, the user is logged in.

When the user logs out, Login Window checks the 802.1X session to determine if it started the session, and if so, it stops the 802.1X session. Also, if it is an 802.11 network, it disassociates from the network.

If no one is logged in, no 802.1X session is running, so no 802.11 network is joined. The Mac is not available on the authenticated network.

This mode is typically of interest to enterprise environments that use managed computing technologies with directory services to remotely administer and manage the computer and user accounts.

You can have multiple Login Window profiles for each location.

## System Profile

In the System mode Snow Leopard authenticates to the network as long as this mode is enabled. That means the computer authenticates to the network even when no one is logged in, regardless of which user account logs in afterwards.

This is useful if the computer needs to be connected to the network regardless of whether anyone is logged in or not.

In computer labs and other similar environments where a system administrator needs to update large groups of computers at the same time, this may be the best method.



You can only have one instance of a System Profile configured for your location. If you add a User or Login Window Profile to the same location, they are ignored—the System Profile has precedence.

### System Profile Plus Login Window Profile

Snow Leopard also provides support for multiple 802.1X profiles. A common example is to define a System profile and a Login Window profile together.

By using this combination of profiles, the computer authenticates through 802.1X at boot using the defined System profile. Then when the user enters a user name and password at the Login Window, those credentials are used to authenticate the user through 802.1X using the defined Login Window profile.

After the user logs out, the computer authenticates using the System profile.

### About Certificates in an 802.1X Environment

802.1X uses a server and client certificate. These certificates must meet specific requirements on the server and on the client for successful authentication.

When you connect to an 802.1X network, you may be presented with a certificate trust dialogue asking if you want to continue with the authentication to the server. In the dialogue, you can select “Always Trust” the certificate, or click “Continue” to authenticate a single time.

Certificates are stored in Keychain Access. All User profile certificates are installed in the Login Keychain section of Keychain Access and all Login Window and System profile certificates are installed in the System Keychain section of Keychain Access.

One purpose of the certificate trust dialogue is to inform you when a server presents a certificate that has not been explicitly trusted. Another purpose is to allow you to examine the certificate to ensure that it is appropriate for the network you are authenticating to.

You should carefully examine certificates and not just blindly accept them. It’s possible for someone to set up a rogue access point with their own certificate, and if you continue with the authentication, the rogue access point could gather your password from the authentication exchanges.

A certificate contains SHA-1 and MD-5 fingerprints, which uniquely identify the certificate. Verify each certificate in the list, and if you are confident in the validity, trust the certificates. If you are unsure, consult with your system administrator before continuing.

When selecting a certificate for your 802.1X configuration, it must be the specific one for access to the RADIUS server you are connecting to.

Some 802.1X networks require you to obtain a certificate of authority. Ask your network administrator how to obtain a 802.1X certificate for your network.

The certificate creation process involves the following:

- Generating a private key and Certificate Signing Request (CSR)
- Providing the CSR to the CA
- CA signing the CSR and issuing the certificate
- Importing the certificate into the keychain to establish the connection between the private key and certificate

There is a distinction between a certificate for which you have the private key, usually referred to as an identity, and just a certificate. A certificate is the public part of public key infrastructure, and allows people to verify that you hold the private key. A private key is only held by the entity that corresponds to the subject of the certificate, and must be stored securely.

It's also possible that you have the identity (certificate + private key) in the form of a PKCS12 (.p12, .pfx) file. This file can be imported into the keychain by double-clicking it.

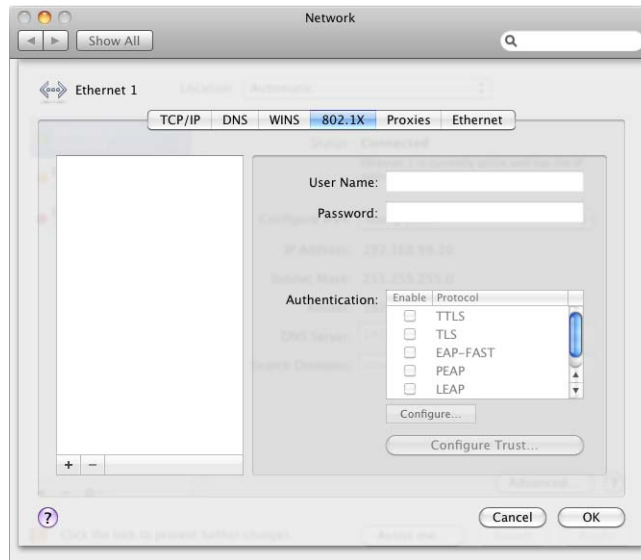
### Extensible Authentication Protocol (EAP) Methods

Snow Leopard supports six EAP methods of authentication, though not all EAP methods are supported across both Ethernet and AirPort interfaces. The following are supported EAP methods of authentication.

- TTLS
- PEAP
- TLS (requires a certificate)
- EAP-FAST
- LEAP
- MD5 (authentication type for wired ethernet connections)

## Connecting to a 802.1X Network

Choose an 802.1X profile and follow the instructions to enter the information in the 802.1X pane of Network preferences (shown below) for the network service you require. An administrator (any user account with administrator level privileges on the computer) can create a valid 802.1X profile.



Although it is not necessary to create a Network location for a User profile, it is helpful in a Login Window and System profile 802.1X configuration. When creating a location, 802.1X profiles that are configured are stored only under that location.

If you create a location, be sure it is selected when you are at that location. For example, when traveling between two office locations, one in New York and one in London, you must select the correct location to connect to the 802.1X network of the office you are visiting.

User profiles are not location-sensitive. They are per user. You can add User profiles as needed.

If you use TLS authentication, before doing anything else you must install a user certificate or private key pair. We recommend that the System Administrator do it.

### To connect to an 802.1X network:

- 1 Connect to your network and use System Preferences > Accounts > Login Options to verify you're connected to an Open Directory or Active Directory server.

You only need to ensure you are connected to a directory server if you use a System or Login Window profile.

- 2 Choose Apple > System Preferences > Network.
- 3 From the Location pop-up menu, select Edit Location.

Click the Add (+) button at the bottom of Locations, create a Location and name it to remind you of where this location is, and then click Done.

It is unnecessary to specify a location if you are setting up a User profile.
- 4 From the network connection services list, select the network service to set up, such as Ethernet or AirPort, and then click Advanced.
- 5 Click the 802.1X tab.
- 6 Click Add (+) button at the bottom of the profiles list, and choose a profile:
  - User Profile
  - Login Window Profile
  - System Profile
- 7 Rename the Untitled profile by double-clicking it and entering a name.
- 8 Enter the user name and password.

If you are using a User or System profile, enter the user name and password supplied by your network administrator for your account. If you are using TLS, a user name and password is unnecessary.

If you are using a Login Window profile, leave the user name and password blank. However, the connection is not affected if you enter the user name and password. You are asked for the user name and password during the initial connection to the server when you click Apply. They are not used again.
- 9 If you are setting up a wireless 802.1X connection, choose a network from the Wireless Network pop-up menu.

If your wireless network name (SSID) is hidden, you must manually enter it. It is case sensitive.
- 10 Select and configure the EAP Authentication types for your network.

The default is PEAP and TTLS.
- 11 Click Configure Trust, then click the Certificate pane.
- 12 Click the Add (+) button and choose "Select Certificate File" or "Select Certificate From Keychain" from the pop-up menu.

If you choose "Select Certificate File," locate the certificate file and click Open.

If you choose "Select Certificate From Keychain," select a certificate from your keychain and click OK.

Certificates you add to the list are always trusted.
- 13 Click the Servers pane.

- 14 Click the Add (+) button and enter the name of the server you want to trust.  
Servers you add to the list are always trusted.
  - 15 Click OK.
  - 16 Click OK to save the profile.
  - 17 Click Apply to save the 802.1X configuration.
  - 18 If you are connecting to an 802.1X WEP based wireless network, do the following to ensure connectivity:
    - a Choose Apple > System Preferences.
    - b Click Network.
    - c Choose AirPort in the network connection services list and then click Advanced.
    - d Click the Add (+) button at the bottom of the list.
    - e Enter the case-sensitive Network Name (SSID).
    - f From the Security pop-up menu, choose 802.1X.
    - g Leave the User Name and Password fields blank.
    - h From the 802.1X pop-up menu, choose the 802.1X profile you created and it will fill in your user name and password.
    - i Click Add.

If a certificate was issued from a nontrusted CA, you are prompted to trust the certificate from the server. When you trust the certificate, a new entry is added to the Login keychain.
  - 19 When prompted, enter your administrator password so you can set the required level of trust on that certificate.
  - 20 To be able to rejoin the network after waking your computer from sleep, verify that the network is selected in the Preferred Networks list (or that the Remember networks option is selected).
  - 21 If 802.1X WEP is used, create an entry in the Preferred Networks list for Login, System, or User profiles to work.
  - 22 If you are setting up a User profile, don't add a Login Window or System profile.  
They take precedence over User profiles.
- For information about importing 802.1X profiles, see the `networksetup` man page.

## Securing Managed User Accounts 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:

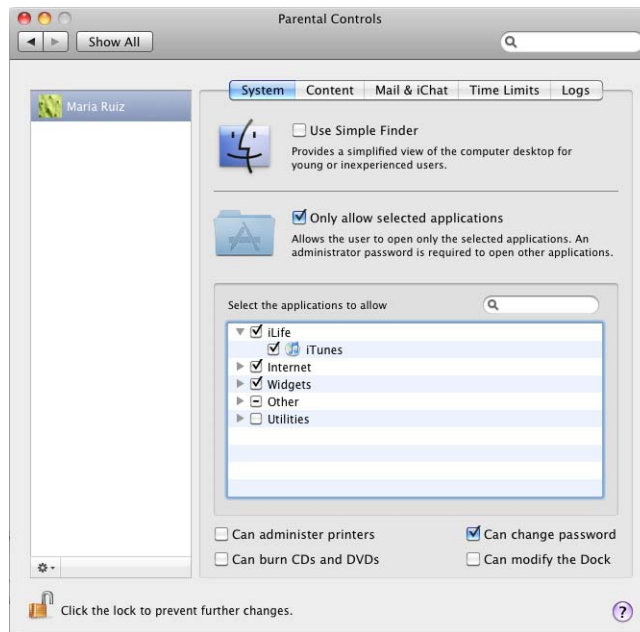
- Only allow selected applications. You can restrict the user's access to specific applications by deselecting the checkbox next to the application in the "Check the applications to allow" list.
- Can administer printers. You can restrict the user's ability to select alternative printers and to change 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 websites that the user can visit.

### To secure Parental Controls preferences:

- 1 Open Parental Controls preferences.

A screen similar to the following appears:

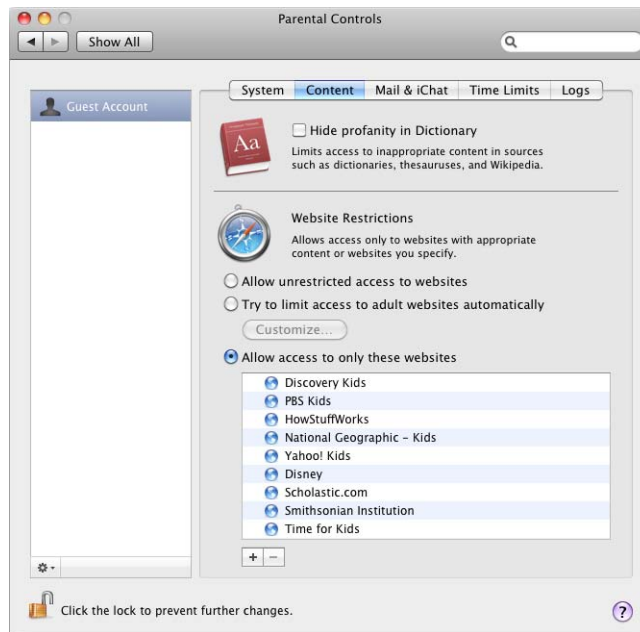


- 2 Select the account you want to activate parental controls for.

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 In the “Select the applications to allow” list, 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.

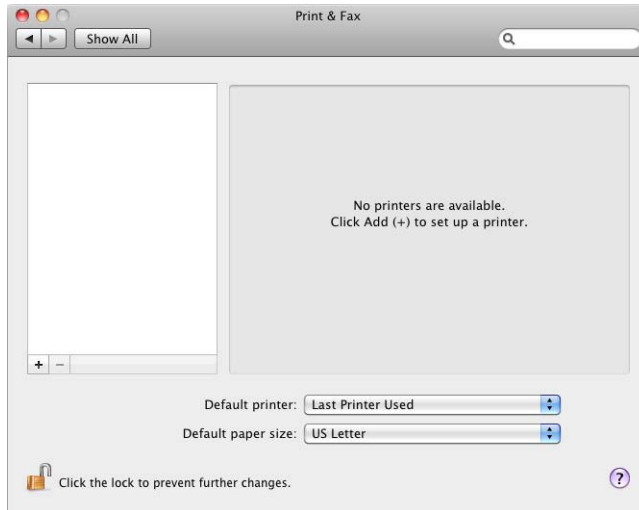
A screen similar to the following appears:



- 7 In the Content pane, limit website access to specific sites by selecting “Allow access to only these websites.”
- 8 Click the Add (+) button, 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>). By default, CUPS web interface 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>.

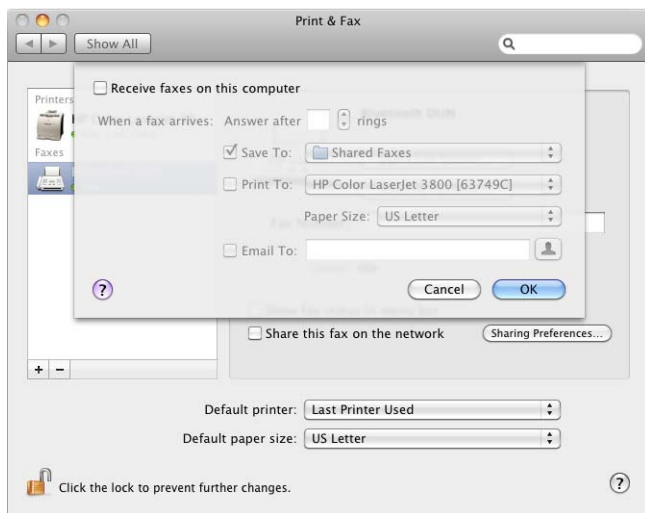
To avoid an additional avenue of attack, don't receive faxes on your computer.



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

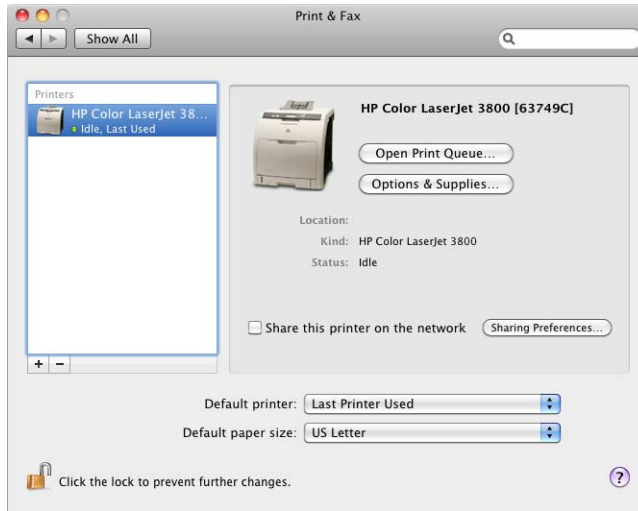
- 1 Open Print & Fax preferences and select a fax from the equipment list.
- 2 Click Receive Options.

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 on the network.”

From the command line:

```
# Securing Print & Fax Preferences
# -----
# Default Setting:
# Disabled

# Suggested Setting:
# Disable the receiving of faxes.
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist
# Disable printer sharing.
sudo 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

# Available Settings:
# Enabled or Disabled
```

## 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). For more information, see "Securing System Swap and Hibernation Storage" on page 104.
- **Location Services:** Disabling location services prevents information about the location of your computer from being provided to applications.
- **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 153.

## Firewall Security

When you start firewall using the Firewall pane, only signed software is allowed to receive incoming connections. Using the advanced section of the firewall (shown here), you can specify which applications are authorized or unauthorized to accept incoming network connections.



**Note:** We recommend that you block all incoming connections and allow only basic Internet services.

Advanced options also include stealth mode that prevents the computer from sending responses to uninvited traffic.

### To securely configure Security preferences:

- 1 Open Security preferences.
- 2 Select the following:
  - “Require password \_\_\_ after sleep or screen saver begins”
  - “Disable automatic login”
  - “Require password to unlock each System Preferences pane”
- 3 Deselect the “Log out after # minutes of inactivity” checkbox.

- 4 Select the "Disable Location Services" checkbox.
- 5 Select the "Disable remote control infrared receiver" checkbox.
- 6 In the FileVault pane, click "Turn on FileVault."
- 7 Enter a password in the Master Password and verify fields.
- 8 Authenticate with your account password.
- 9 Select "Use secure erase" and click "Turn on FileVault."
- 10 In the Firewall pane, click Start.
- 11 If needed, click "Advanced" and select "Enable Stealth Mode" and "Block all incoming connections."
- 12 Add specific services and applications to the list and set them to allow or block incoming connections.
- 13 Restart the computer.

From the command line:

```
# Securing Security Preferences
# -----
# Default Setting:
# Required Password Wake: Disabled
# Automatic Login: Disabled
# Password Unlock Preferences: Disabled
# Secure Virtual Memory is Enabled on Portable computer and is Disabled
# on Desktop computers.
# IR remote control: Enabled
# FileVault: Disabled

# Suggested Setting:
# Enable Require password to wake this computer from sleep or screen saver.
sudo defaults -currentHost write com.apple.screensaver askForPassword -int
    1
# Disable Automatic login.
sudo defaults write /Library/Preferences/.GlobalPreferences\
com.apple.userspref.DisableAutoLogin -bool yes
# Require 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.
sudo defaults write /Library/Preferences/.GlobalPreferences\
com.apple.autologout.AutoLogOutDelay -int 0
# Enable secure virtual memory.
sudo defaults write /Library/Preferences/com.apple.virtualMemory\
    UseEncryptedSwap -bool yes
# Disable IR remote control.
sudo defaults write /Library/Preferences/com.apple.driver.AppleIRController
    DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
sudo /System/Library/CoreServices/ManagedClient.app/Contents/Resources/\
createmobileaccount
# Enable Firewall.
# Replace value with
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
sudo defaults write /Library/Preferences/com.apple.alf globalstate -int
    value
# Enable Stealth mode.
sudo defaults write /Library/Preferences/com.apple.alf stealthenabled 1
# Enable Firewall Logging.
sudo defaults write /Library/Preferences/com.apple.alf loggingenabled 1
```

## Securing System Swap and Hibernation Storage

The data that an application writes to RAM might contain sensitive information, such as user names and passwords. Snow Leopard 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.

When your computer is turned off, information stored in RAM is lost, but information stored by virtual memory in a swap file may remain on your hard disk in unencrypted form. The Snow Leopard virtual memory system creates this swap file 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).

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 disk.

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
# -----
# Default Setting:
# Secure Virtual Memory on Portable computers is Enabled and is Disabled on
# Desktop computers.

# Suggested Setting:
# Enable secure virtual memory.
sudo defaults write /Library/Preferences/com.apple.virtualMemory\
    UseEncryptedSwap -bool YES

# Available Setting:
# UseEncryptedSwap -bool NO
# UseEncryptedSwap -bool YES
# You can also turn hibernate off by using the following command:
# sudo pmset hibernatemode 0
```

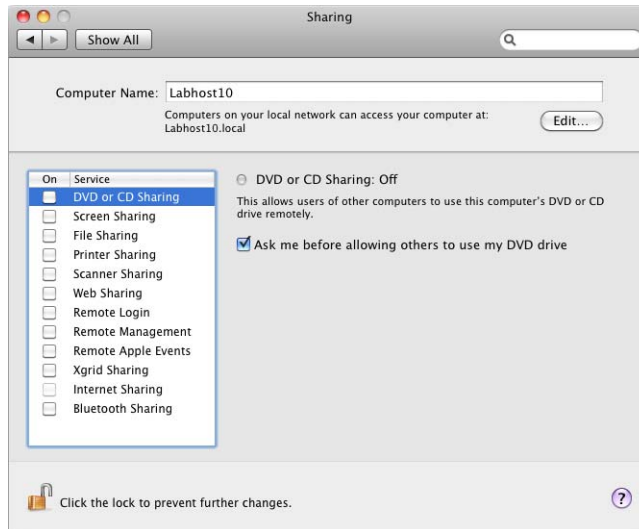
## Securing Sharing Preferences

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 199.

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.
Scanner Sharing	Allows other users to use a scanner 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.

Service	Description
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 9, "Securing Network 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
# -----
# Default Setting:
# $host_name = User's Computer

# Suggested Setting:
# Change computer name where $host_name is the name of the computer.
sudo systemsetup -setcomputername $host_name
# Change computer Bonjour host name.
sudo scutil --set LocalHostName $host_name

# Available Setting:
# The host name cannot contain spaces or other non-DNS characters.
```

## 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 38.

After transferring installer packages to your computer, verify the authenticity of the installer packages. For more information, see "Repairing Disk Permissions" on page 40.

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
# -----
# Default Setting:
# Check for Updates: Enabled
# Check Updates: Weekly

# Suggested Setting:
# Disable check for updates and Download important updates automatically.
sudo softwareupdate --schedule off

# Available Setting:
# Check for Updates: Enabled or Disabled
# Check Updates: Daily, Weekly, Monthly
```

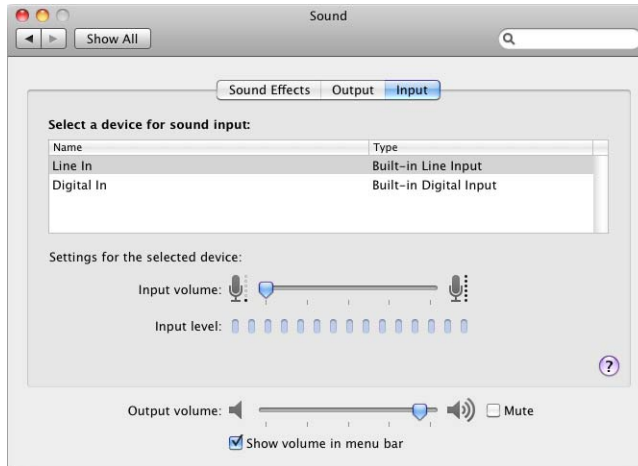
## Securing Sound Preferences

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
# -----
# Default Setting:
# Internal microphone or line-in: Enabled

# Suggested Setting:
# Disable internal microphone or line-in.
# This command does not change the input volume for input devices. It
# only sets the default input device volume to zero.
sudo osascript -e "set volume input volume 0"

# Available Setting:
# Internal microphone or line-in: Enabled or Disabled
```

## Securing Speech Preferences

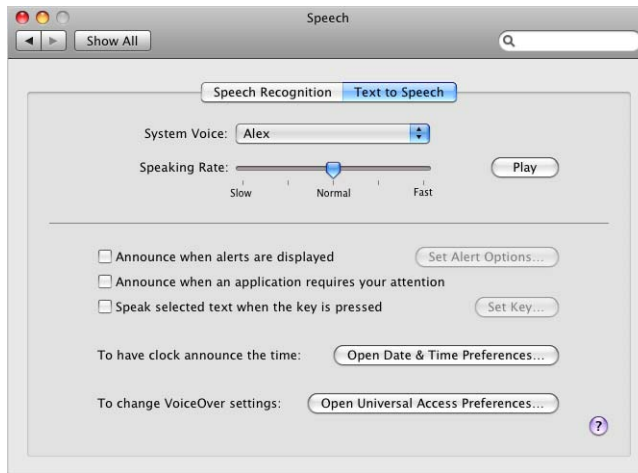
Mac OS X includes speech recognition and text-to-speech features, which are disabled by default.

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
# -----
# Default Setting:
# Speech Recognition: Disabled
# Text to Speech: Enabled

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

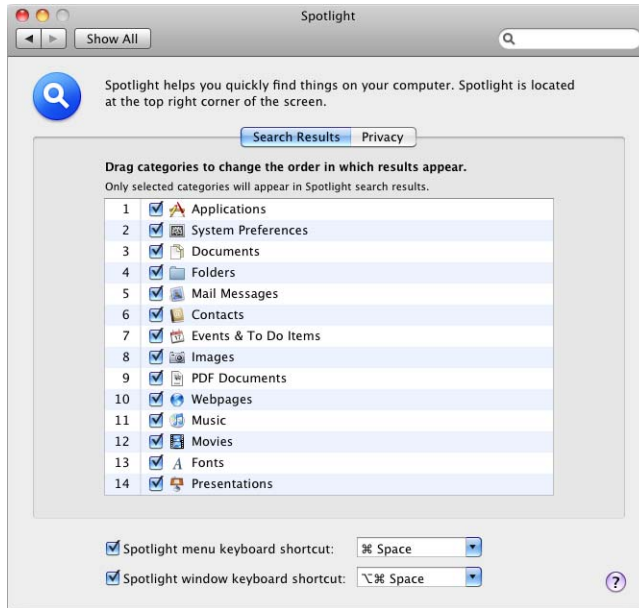
# Available Setting:
# Each item can be set to ON or OFF:
# OFF: -bool false
# ON: -bool true
```

## Securing Spotlight Preferences

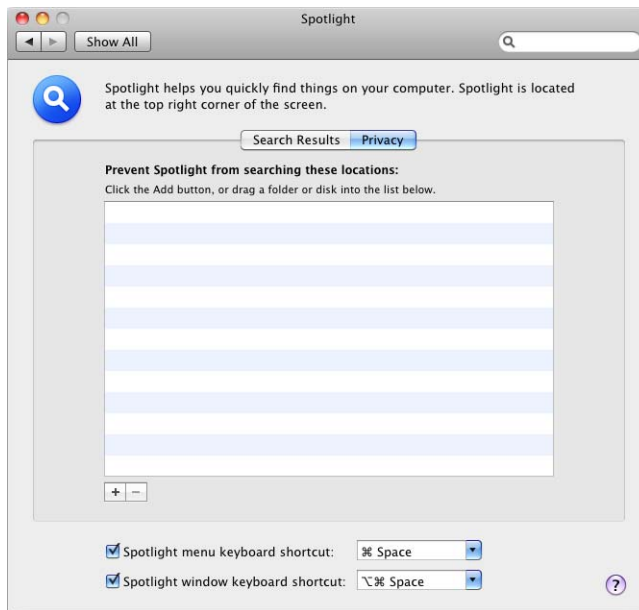
You can use Spotlight to search your computer for files. Spotlight searches the name, the meta-information associated with each file, and the contents of each file.

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 40.

The following is the 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
# -----
# Default Setting:
# ON for all volumes

# Suggested Setting:
# Disable Spotlight for a volume and erase its current meta data, where
# $volumename is the name of the volume.
sudo mdutil -E -i off $volumename

# Available Setting:
# Spotlight can be turned ON or OFF for each volume.
```

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 43.

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 EFI password. If you enable an EFI password, you can still restart in Target Disk Mode using Startup Disk preferences.

For more information about enabling an EFI password, see “Using the Firmware Password Utility” on page 55.

**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
# -----
# Default Setting:
# Startup Disk = “Macintosh HD”

# Suggested Setting:
# Set startup disk.
sudo systemsetup -setstartupdisk $path

# Available Setting:
# Startup Disk = Valid Boot Volume
```

## 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
# -----
# Default Setting:
# OFF

# Suggested Setting:
# Enable Time Machine.
sudo defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1

# Available Setting:
# 0 (OFF) or 1 (ON)
```

## Securing Universal Access Preferences

Universal Access preferences are disabled by default. 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.

From the command line:

```
# Securing Universal Access Preferences
# -----
# Default Setting:
# OFF

# Suggested Setting:
# Disable VoiceOver service.
launchctl unload -w /System/Library/LaunchAgents/com.apple.VoiceOver.plist
launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.ScreenReaderUIServer.plist
launchctl unload -w /System/Library/LaunchAgents/com.apple.scrod.plist

# Available Setting:
# None
```

Use this chapter to learn how to secure accounts by assigning user account types, configuring directory access, using strong authentication procedures, and 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 is disabled by default because it does not require a password to log in to the computer. The guest account should remain disabled. If this account is enabled and 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 enable the guest account, enable parental controls to limit what the user can do. Enabling parental control on an account does not defend against a determined attacker and should not be used as the primary security mechanism.

Whether or not the guest account 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 121.

## 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.

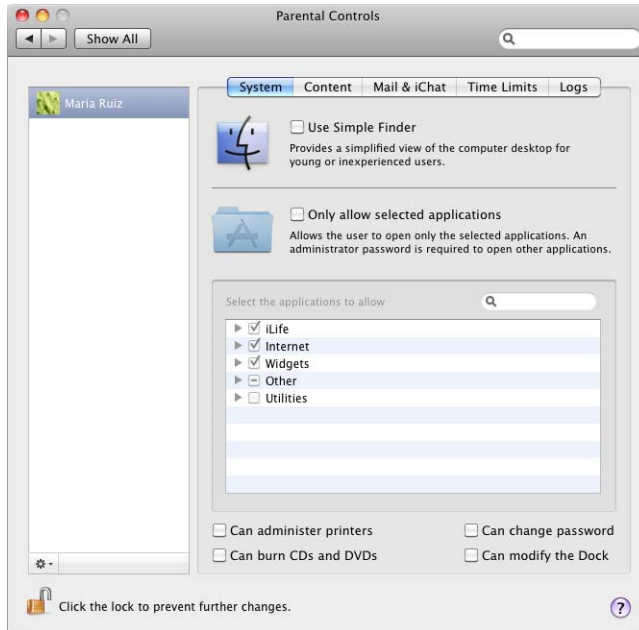
**Note:** If your computer is connected to a network, a managed user can also be a user whose preferences and account information are managed through the network.

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, Snow Leopard 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 Snow 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

A directory-based account is an account 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 nonadministrative account should be used for most daily activity, especially when accessing the network or Internet.

The administrator's account should be used 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. 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.”

If the root account is enabled, you can disable it 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 only 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, later `sudo` commands are limited to the terminal where 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.

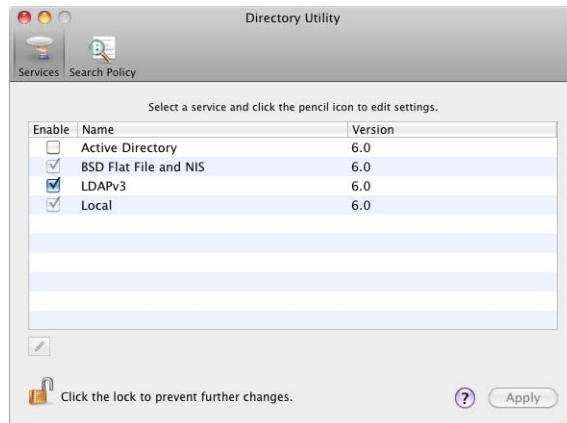
Users with mobile accounts have local and network home folders that combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders. For information about protecting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

## Understanding Network Services, Authentication, and Contacts

You can use Account preferences to configure your computer to use a network-based directory domain. For advanced connections or modifications, use Directory Utility.

Directory Utility can be accessed from Account preferences by clicking Login Options and then clicking Join or Edit and then clicking Open Directory Utility.

In Directory Utility, you can disable directory search services that are not used by deselecting them in the Services pane (shown here).



You can also enable or disable each kind of directory service protocol.

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 v10.6 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.

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 v10.6 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 v10.6 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

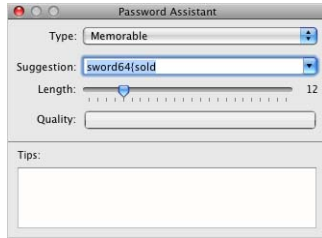
Snow Leopard includes Password Assistant, an application that analyzes the complexity of a password or generates a complex password for you. You can specify the length and type of password you'd like to generate.

You can choose from the following types of passwords:

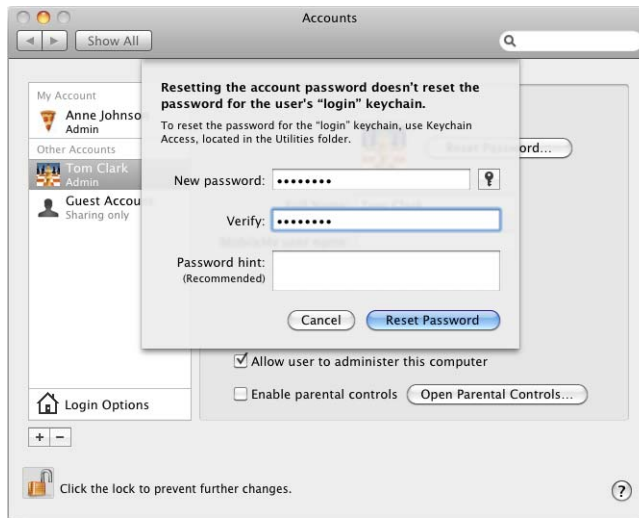
- **Manual:** You enter a password and then Password Assistant gives you the quality level of your password. If the quality level is low, Password Assistant gives tips for increasing the quality level.
- **Memorable:** According to your password length requirements, Password Assistant generates a list 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:** Snow Leopard supports Kerberos v5 but does not support Kerberos v4.

Snow 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 Snow 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 Snow Leopard 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 supplying 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 198.

Normally, after your computer gains a Kerberos ticket in this manner, keep the Kerberos ticket until it expires. However, you can manually remove your Kerberos ticket using the Kerberos utility in Snow Leopard.

**To manually remove a Kerberos ticket:**

- 1 Open Keychain Access (in /Applications/Utilities).
- 2 From the Keychain Access menu, choose 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 Ticket” to delete that key.

You can also use the `kinit`, `kdestroy`, and `kpasswd` commands to manage Kerberos tickets. For more information, see the `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 Snow 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/business/resources/](http://www.apple.com/business/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 enhance 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.

Snow Leopard 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 130.

- 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 137.

## 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 137.

## 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 select “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

Snow 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 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 to view the PIN-protected data on that smart card.

For more information, see the *Smart Card Setup Guide* at [www.apple.com/business/resources/](http://www.apple.com/business/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 157.

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 162.
- 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 Snow Leopard, 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, Snow Leopard 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, and 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. Although 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 CA 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 CA. Use the 2048 bit key size when you create your certificate.

By default, certificates created using Certificate Assistant have a 2048 bit key size. Keys less than 1024 bits are known to be broken, and 1024 bit keys are expected to be broken within the expiration time of the certificate issued.

### **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.
- 4 From the Identity Type pop-up menu, choose one of the following:
  - Self-signed root certificate: A self-signed root certificate is a root CA 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. However, they are easy and quick to make, and are often used for testing purposes in place of certificates signed by proper CA.
  - Leaf certificate: A leaf is a certificate signed by an intermediate or root CA. A leaf certificate benefits from the security of certificate chains and certificate policies. A leaf is situated at the bottom of a certificate chain.
- 5 From the Certificate Type pop-up menu, choose the specific purpose that your certificate will be used for.
- 6 If you want to manually specify the information in the certificate, such as key pairs, extensions, and encryption, select “Let me override defaults.”
- 7 Click Continue.
- 8 When prompted “You are about to create a self-signed certificate,” click Continue.
- 9 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. After 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 Add.
- 4 If you're asked to provide a name and password, enter 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 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 *User Management*.
- **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 Sharing & 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` (`rx`) 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 `rx` 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 kernel security level (`kern.securelevel`) is less than or equal to zero. To determine your current kernel security level, use this command `sysctl kern.securelevel`.

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 new 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 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 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 runs 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 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 for many programs on the system to perform the specific, privileged tasks they are designed for. The ping program, for example, is `setuid` because it must 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`.

Snow Leopard 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 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
/usr/bin/at	Job Scheduler
/usr/bin/atq	Job Scheduler
/usr/bin/atrm	Job Scheduler
/usr/bin/crontab	Job Scheduler
/usr/bin/postdrop	Postfix Mail
/System/Library/PrivateFrameworks/DesktopServicesPriv.framework/Versions/A/Resources/Locum	Performing Privileged File Operations using Finder

Application	Related Service
/usr/bin/postqueue	Postfix Mail Queue
/usr/bin/procmail	Mail Processor
/usr/bin/wall	User Messaging
/usr/bin/write	User Messaging
/usr/bin/chrfn	Change Finger Information
/System/Library/Printers/IOMs/LPRIOM.plugin/ Contents/MacOS/LPRIOMHelper	Printing
/usr/sbin/traceroute	Trace Network Path
/usr/sbin/traceroute6	Trace Network Path
/sbin/mount_fs	Mounting NFS Filesystems
/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/scselect	Allowing non-administrators to change Network Location

**Important:** The Repair Permissions feature of Disk Utility reenables the setuid bit on these programs. Software updates may also reenables the setuid bit on these programs. To achieve some persistence for the permissions change, create a shell script to strip the bits and then implement a launchd 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 launchd job, see *Introduction to Command-Line Administration*, available at [www.apple.com/server/macosx/resources/](http://www.apple.com/server/macosx/resources/).

### Using ACLs to Restrict Usage of Setuid Programs

You can also use the ACL feature of Snow Leopard 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 have 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 following commands 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 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. To achieve a degree of persistence for the ACLs, create a shell script to set the ACLs and then implement a launchd job (for the root account) to execute this script.

For information about how to set up a launchd job, consult *Introduction to Command-Line Administration*, available at <http://www.apple.com/server/macosx/resources/>.

A launchd job should ensure that a specific time period (or less) 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 noncanonical 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, permissions on the home folder of a 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-writable permissions if File Sharing or Web Sharing is enabled. If these services are not in use, 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 Snow 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 disables 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. Snow Leopard supports the Mac OS X version 10.4 Tiger sparse disk image format created using AES-128 encryption. 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 157.

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 162.

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 must encrypt specific files or folders. FileVault can only be enabled for local or mobile accounts and cannot be enabled for network home folders.

To protect files or folders on portable media or a network volume, create an encrypted disk image on the portable media or network volume. Then mount these encrypted disk images, which protect data transmitted over the network using AES-256 encryption. When using this method, 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 157.

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 130.

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

Snow 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 of centralized management of FileVault on a client computer is to use Snow 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 Set 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 130.

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 In the Name field, enter the name you want to appear when the image is mounted.
- 5 Choose the size of the image from 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.
- 6 Choose a format from the Format pop-up menu.

- 7 Choose an encryption method from the Encryption pop-up menu.  
AES-128 or AES-256 is a strong encryption format.
- 8 Choose a partition type from the Partitions pop-up menu.  
The default is Single partition - Apple Partition Map.
- 9 Choose a format from the Image 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.
- 10 Click Create.
- 11 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 130.
- 12 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 157.

#### 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 Enter a name for the image and choose where to store it.
- 5 Choose a format from the Image Format pop-up menu.  
The compressed disk image format can help you save hard disk space by reducing your disk image size.
- 6 Choose an encryption method from the Encryption pop-up menu.  
AES-128 or AES-256 provide strong encryption.
- 7 Click Save.
- 8 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 130.

- 9 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. Also, using an encrypted disk image is more secure than using an encrypted PDF.

Some applications do not support printing to PDF. In this case, create an encrypted disk image. For information, see “Creating an Encrypted Disk Image from Existing Data” on page 158.

### 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 documentWhen 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 Snow 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 Secure Empty Trash.

## 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.

## Securing 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, 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 Snow Leopard. This prevents your sensitive data from being accessed by the guest operating system. For more information, see "Creating an Encrypted Disk Image" on page 157.

Also, keep backup copies of your data in the event that your Snow Leopard partition becomes corrupt.

When setting a password for your guest operating system, start in Snow Leopard and use Password Assistant to create a strong password. For more information, see "Using Password Assistant to Generate or Analyze Passwords" on page 130.

You can also prevent attacks by keeping your guest operating system installed with the most current updates.

## Understanding the Time Machine Architecture

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.

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 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 157.
- 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.

### Setting 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 receive 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 Encrypted (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. Snow 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 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
- Kerberos Version 5 (GSSAPI)
- NTLM

**Note:** Password is the default selection. Using Password for this option does not provide additional authentication or password protection.

The authentication method you choose should match the configuration of the mail server for the account being established. The server and the client must be configured with the same authentication method 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 SMTP 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
  - Kerberos Version 5 (GSSAPI)
  - NTLM
- 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 messages between client and server. However, these precautions cannot guarantee that the sender is not malicious. Users should never open attachments from unknown senders, and should not display remote content from senders without 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. This should be changed to display the email address of the sender.

Also, the default for Mail is to display remote images in HTML messages. Because 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.

### Disabling the Preview Pane for Mail Messages

To completely avoid viewing messages from malicious senders, disable the message preview pane. After it is disabled, messages must be double-clicked 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 message.
- 2 Double-click the separator bar.

It should move to the bottom of the window and remain there.

After the Review pane is disabled, the user must double-click each message to open and view it. 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 that has 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 Encrypted (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 Encrypted 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.

## Setting 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 not 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). Some websites have extended validation certificates, also known as EV certificates, which require more extensive investigation by the certifying agencies. Safari supports EV certificates.

There are two common methods for verifying the validity of a certificate: Online Certificate Status Protocol (OCSP) and Certificate Revocation List (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 verify certificates you receive.

OCSP and CRL are off by default. To change the validation settings, use Keychain Access > Preferences, and then click Certificates.

You can also visually inspect certificates using Safari or Keychain Access.

Safari warns you if a certificate is invalid. If a certificate warning appears, do not proceed to the site. If you continue to the site, your secret information can be exposed. If you encounter a certificate warning, contact the administrator of the site you are attempting to visit and let them know.

You can also manually 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 also 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, 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 an 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 (certificate chain validation only).”
- To evaluate Code Signing, select “Code Signing.”

## 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 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 CA who issued the certificate.

## Managing Data Communication and Execution

Safari and Snow Leopard tag every download with the extended attribute `com.apple.quarantine`. The attribute contains information about when and where it was downloaded. When you attempt to open a downloaded application, Snow Leopard reminds you where it came from before opening it for the first time, so you can be sure it’s legitimate.

## 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 Snow 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.

When you attempt to open a quarantined file, the file is also checked for known instances of malware software. If malware software is discovered, a warning appears. Click the Move to Trash button to delete the file. If it is a disk image, eject the image and delete the source file.

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. For example, if the protocol being used to send the forms does not use encryption or uses clear text, Safari will consider it nonsecure and display a message.

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 Snow 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 "Synchronize bookmarks using MobileMe." 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.

From the command line:

```
# -----  
# Securing Applications  
# -----  
# Disabling iSync  
# -----  
# Default Setting:  
# OFF  
  
# Suggested Setting:  
# Disable iSync.  
launchctl unload -w /System/Library/LaunchAgents/  
    com.apple.syncservices.SyncServer.plist  
launchctl unload -w /System/Library/LaunchAgents/  
    com.apple.syncservices.uihandler.plist  
  
# Available Setting:  
# None
```

For more information about using `launchctl`, see “Understanding and Managing Daemons and Agents” on page 221.

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 don't want to save the information yet. 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.

You can disable plug-ins by removing them from the /Library/Internet Plug-Ins/ folder.

The Java plug-in is enabled by default and handles Java applets on webpages. If you are not using Java, disable the Java plug-in.

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.

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.

### To disable plug-ins and block pop-ups:

- 1 Open Safari
- 2 Click Safari > Preferences.
- 3 Click Security.



- 4 Deselect the Enable plug-ins checkbox and the Block pop-up windows checkbox.  
A warning appears explaining information you may miss when you block pop-ups, when you deselect the Block pop-up windows checkbox.
- 5 Close Safari preferences.

## 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), Snow Leopard 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 Snow Leopard 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 you open a quarantined file, the file is also checked for known instances of malware software. If malware software is discovered, a warning appears. Click the Move to Trash button to delete the file. If it is a disk image, eject the image and delete the source file.

When distinguishing between legitimate and malicious applications, the most important indicator is where you get the file from. 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.

## Using Instant Message Security with iChat

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. Although iChat can be configured with security, disable it unless your organization requires messaging services.

You can set up secure iChat messaging using your MobileMe membership. However, 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 can't 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 140.

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* and *iChat Server 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. To prevent unauthorized users from instant messaging you, you can reject their request to send you messages.

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 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 Snow Leopard 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.

## Enhancing 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 130.

## Setting Photo Sharing Security with 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.

## Setting Contact Sharing Security with 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.

## Strengthening Data Security with MobileMe

By using MobileMe you stay connected to your data when you are away from your computer. In sensitive environments don't use MobileMe. When accessing MobileMe data, make sure you are using a secure network connection and that you encrypt the data you transfer.

### 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 to access 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.

## 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.

Your Snow 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 Internet Communication with Host-Based Firewalls

Using a firewall to filter network traffic from 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.

Snow Leopard 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, click Advanced in the Firewall pane of Security preferences. Then click the Add (+) button at the bottom of the list and select the application. 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.

## The Application Firewall

Snow 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

When the Application Firewall is off, Snow Leopard does not block incoming connections to your computer. This is the default mode for Snow Leopard. If you upgraded from Mac OS X v10.4, your Application firewall defaults to this mode.

When you turn the Application firewall on, the firewall prevents unauthorized applications and services from accepting incoming connections.

The Application firewall has the following modes of operation:

- *Block all incoming connections:* This is the most conservative mode. Snow Leopard blocks 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:

- **config:** Implements DHCP and other network configuration services.
- **mDNSResponder:** Implements Bonjour.
- **racoon:** Implements Internet Key Exchange (IKE).
- *Automatically allow signed software to receive incoming connections:* This mode is set by default. Applications signed by a valid certificate authority are allowed to provide services accessed from the network.
- *Enable stealth mode:* This mode prevents your computer from responding to ICMP ping requests and hides it from unwanted network scans.

You can also manually set access for specific services and applications by choosing 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, Snow Leopard digitally signs the application (if it is not 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.

## 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 If 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 are digitally signed by a trusted CA (for the purpose of code signing) can receive incoming connections. Every Apple application in Snow Leopard is 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, Snow Leopard signs the application and adds it to the Application Firewall list. If you choose Deny, Snow 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

Snow 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 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 designed to match packets and take appropriate action. IPFW rules are numbered from 1 to 65535. The packet passed to the firewall is compared to each rule (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 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 is 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 been added to the system, packets are passed to this default rule, which allows them through. However, if Stealth Mode is enabled on the system, the following line appears first in the list:

```
33300 deny icmp from any to me in icmp types 8
```

This rule shows the implementation of Stealth Mode: 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.

Except for Stealth Mode blocking ping requests, the default configuration for IPFW on Snow Leopard does not block packets. Snow Leopard 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.

## 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 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

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 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, logging is enabled for the Application Firewall and IPFW. The system sends 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 connectivity failures.

## Implementing a Basic Inclusive Ruleset

An IPFW ruleset can be stored 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 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 to allow responses
add 10000 allow tcp from any to any out keep-state
#Allow all UDP packets out, and keep state 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 is dropped and logged
add 65534 deny log ip from any to any
#Allow all IP packets: here as a reminder of the default rule
#65535 allow ip from any to any
```

When 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 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 new rules are inserted.

To flush old rules and re-insert a ruleset from `/etc/ipfw.conf`, enter the following:

```
$ sudo /sbin/ipfw flush
$ sudo /sbin/ipfw /etc/ipfw.conf
```

To verify that the rules in `/etc/ipfw.conf` are loaded at startup, see “Configuring the System to Load the IPFW Ruleset” on page 192. Even if DHCP is not used, unconnected interfaces can create log messages when they attempt to obtain IP settings from the computer. To eliminate messages, configure the interfaces to “Off” using the Network preference pane.

## Opening the Basic Ruleset to Permit Services

The basic ruleset does not permit the system to host 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.

Rules should only be added if the system needs to offer the network services discussed. Not all possible network services are 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 Web Sharing, 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 can be made more restrictive by making it specifically drop some types of packets.

For example, 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 other ICMP types are 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 enables Stealth Mode, because 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 takes precedence because it 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 does not have packet fragmentation, fragmented packets can be a sign of abnormal activity. The following rule drops 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 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 load.

## 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 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 LAN.

## VPN Security

There are three encrypted transport protocols: Layer Two Tunneling Protocol and Secure Internet Protocol (L2TP/IPSec), Point-to-Point Tunneling Protocol (PPTP), and Cisco IPSec.



### About L2TP/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 L2TP, 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 Snow Leopard Server's preferred VPN protocol because it has superior transport encryption and can be authenticated using Kerberos.

### About PPTP

PPTP is a commonly used Windows standard VPN protocol. PPTP offers good encryption (if strong passwords are used) and supports a number of authentication schemes. It uses the user-password to produce an encryption key.

By default, PPTP supports 128-bit (strong) encryption. PPTP also supports the 40-bit (weak) security encryption.

PPTP is necessary if you have Windows clients with versions earlier than Windows XP or if you have Mac OS X v10.2 clients or earlier.

### About Cisco IPSec

VPN support in Snow Leopard was enhanced with the addition of Cisco IPSec. Previously, IPSec was utilized by L2TP, but was not a directly configurable service. Cisco IPSec support in Snow Leopard provides support for Machine Authentication using a shared secret or x.509 identity with the association to Groups.

L2TP/IPSec and Cisco IPSec provide the highest level of security because they use IPSec. PPTP does not use IPSec, which makes it less secure.

#### **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," "PPTP," or "Cisco IPSec" 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.

From the command line:

```
# -----  
# Securing Network Services  
# -----  
# Disabling IKE VPN Key Management Service  
# -----  
# Default Setting:  
# OFF  
  
# Suggested Setting:  
# If a VPN is not used, disable the IKE VPN key management service.  
sudo launchctl unload -w /System/Library/LaunchDaemons/  
com.apple.racoon.plist  
  
# Available Setting:  
# None
```

For more information about `launchctl`, see “Understanding and Managing Daemons and Agents” on page 221.

## 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 to access your system. However, Bonjour mitigates these risks by implementing sandboxing.

To reduce the security risk of running Bonjour, connect only to secure, trusted local networks. 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.

If you cannot trust all services on your local network, do not use Bonjour.

**WARNING:** Carefully follow these steps to disable Bonjour. A malformed or problematic mDNSResponder.plist file can prevent your Mac from starting up. Use Time Machine to perform a full backup of your computer before proceeding.

**To disable Bonjour advertising, enter the following commands:**

- 1 Make a backup copy of the mDNSResponder.plist file.
- 2 Open Terminal and open the mDNSResponder.plist file using your preferred text editor.

For example:

```
sudo vi "/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist"
```

- 3 In the ProgramArguments key of the plist file, add the following string to the <array>...</array> section.

```
<string>-NoMulticastAdvertisements</string>
```

For example:

```
<key>ProgramArguments</key>
  <array>
    <string>/usr/sbin/mDNSResponder</string>
    <string>-launchd</string>
    <string>-NoMulticastAdvertisements</string>
  </array>
```

- 4 Save the changes to the mDNSResponder.plist file.

**Important:** If you edited the file using emacs, remove the emacs backup file (the file with a tilde at the end of the name, "/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist~") or your Mac will not start up.

Also, block Bonjour from listening and accepting Bonjour traffic by creating a firewall rule using `ipfw`. This prevents your computer from receiving potentially malicious Bonjour traffic from the network. If you haven't set up IPFW to run when the computer starts up, see "Configuring the System to Load the IPFW Ruleset" on page 192.

Add the following rule to the `/etc/ipfw.conf` in the same way that you edited `/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist` in the section above.

#### To block Bonjour listening:

```
# Block Bonjour listening
# -----
# Default Setting:
# Bonjour is enabled.
# Firewall is disabled.

# Suggested Setting:
# Add the following line to /etc/ipfw.conf.
add 00001 deny udp from any to me dst-port 5353
# Reload the firewall rules.
sudo /sbin/ipfw flush
sudo /sbin/ipfw /etc/ipfw.conf

# Available Settings:
# Disable firewall and allow Bonjour.
# Enable firewall and block port 5353.
```

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 needed by the user, remove the `<string>-NoMulticastAdvertisements</string>` from the `mDNSResponder.plist` file. Then unblock UDP port 5353 on your firewall.

## To reenable Bonjour broadcast:

```
# Enable Bonjour Service
# -----
# Default Setting:
# Bonjour is enabled
# Firewall is disabled

# Suggested Setting:
# Remove the following line from /etc/ipfw.conf.
add 00001 deny udp from any to me dst-port 5353
# Reload the firewall rules
sudo /sbin/ipfw flush
sudo /sbin/ipfw /etc/ipfw.conf

# Available Settings:
# Disable Firewall and allow Bonjour
# Enable Firewall and block port 5353
```

Some applications can share data such as contact information, photos, and music. When these application share data, they use Bonjour to let other network users know what you are sharing. When you share information, use Password Assistant to help you create a strong password. For information on securing applications that use Bonjour, see Chapter 8, “Securing Applications.”

## Securing the Back to My Mac (BTMM) Service

The new Back to My Mac (BTMM) feature in Snow Leopard gives you access to other computers over the Internet. BTMM requires 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.

By default, BTMM is disabled. Also, the computer cannot be reached until sharing services are enabled in Sharing preferences. Like any other service, keep BTMM disabled unless it is required.

Although BTMM provides a way to set up a secure connection, this service introduces risk, as described in this section. If BTMM is required, its use should be weighed against the security risks it can introduce.

**Note:** Using BTMM, you can only connect to computers that are running Snow 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. Sharing services must be configured carefully to mitigate risk, because 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, choose a strong password and keep it safe. 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 \_\_\_ after sleep or screen saver begins" checkbox and choose a time interval from the pop-up menu.
- 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.

Perform 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 prevent access by 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.

### About DVD or CD Sharing

Data transmitted between computers is not encrypted or secure, so 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.

By default, DVD or CD Sharing is turned off and should be off when it is not used. This prevents unauthorized users from accessing your computer.

**From the command line:**

```
# DVD or CD Sharing
# -----
# Default Setting:
# Disabled (unload)

# Suggested Setting:
# Disable DVD or CD Sharing.
sudo launchctl unload -w /System/Library/LaunchDaemons\
    com.apple.ODSAgent.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)
```

## 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 only use this service in a secure environment.

By default, Screen Sharing is turned off and should be off when it is not used. This prevents unauthorized users from accessing to 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 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 required when attempting to access the computer. Use Password Assistant to create a strong password.

**From the command line:**

```
# Screen Sharing (VNC)
# -----
# Default Setting:
# Disabled

# Suggested Setting:
# Disable Screen Sharing.
sudo srm /private/etc/ScreenSharing.launchd

# Available Settings:
# Enabled:
# "All Users"
# "Only these users"
```



For more information about `launchctl`, see “Understanding and Managing Daemons and Agents” on page 221.

## 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 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 using AFP, user names and passwords are encrypted when the user authenticates to your computer to access files. When using SMB, 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.

By default, File sharing is turned off and should remain off when it is not 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.
# -----
# Default Setting:
# File Sharing Disabled:
# AFP
# FTP
# SMB
# NFS

# Suggested Setting:
# Disable FTP.
sudo launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
# Disable SMB.
sudo defaults delete /Library/Preferences/SystemConfiguration/\
    com.apple.smb.server EnabledServices
sudo launchctl unload -w /System/Library/LaunchDaemons/nmbd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/smbd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smb.server.preferences.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smb.sharepoints.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smbfs_load_kext.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    org.samba.winbindd.plist
# Disable AFP.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.AppleFileServer.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.afpfs_afpLoad.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.afpfs_checkafp.plist
# Disable NFS
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.nfsd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.lockd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.statd.notify.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.portmap.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)
```

For more information about `launchctl`, see “Understanding and Managing Daemons and Agents” on page 221.

## Printer Sharing (CUPS)

Printer Sharing allows users on other computers to access printers connected to your computer. Make sure this service remains disabled unless it is necessary. If it is necessary, 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.

## Scanner Sharing

Sharing allows users on other computers to access scanners connected to your computer. Make sure this service remains disabled unless it is necessary. If it is necessary, consider using dedicated scanner computers instead of sharing a scanner from your computer. By using a dedicated scanner computer, you won’t have scanner traffic routed through your computer.

## Web Sharing (HTTP)

You can use the Apache web server software included with Snow Leopard to host a website on your computer. By default, Web sharing is off and should remain disabled unless it is necessary. Some risks of Web Sharing are described below.

### Web Sharing

Two websites are 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 Web Sharing is running:

`http://your.computer.address`

From the command line:

```
# Web Sharing
# -----
# Default Setting:
# Web Services: Disabled

# Suggested Setting:
# Disable Web Sharing.
sudo launchctl unload -w /System/Library/LaunchDaemons/
    org.apache.httpd.plist

# Available Settings:
# Web Services:
# Disabled
# Enabled
```

## 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 206.

By default, Remote Login is turned off and should remain off when it is not 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)
# -----
# Default Setting:
# Remote Login (SSH): Disabled

# Suggested Setting:
# Disable Remote Login.
sudo launchctl unload -w /System/Library/LaunchDaemons/ssh.plist

# Available Settings:
# Remote Login (SSH):
# Disabled
# Enabled
```

## Enabling an SSH Connection

To set up a system as an SSH server, you must enable Remote Login in Sharing preferences. For more information, see “Securing Sharing Preferences” on page 105.

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 206.

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, when prompted for a location to store the keys, press Enter without entering a location.

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, when prompted for a passphrase, enter a complex password.

A complex password is at least 12 letters 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 130.

- 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, 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 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
#PermitRootLogin yes	PermitRootLogin no	Prevents logging in as root through SSH. Set this for all SSH methods of authenticating.
#PasswordAuthentication yes	PasswordAuthentication no	Disables password authentication.
#PermitEmptyPasswords no	PermitEmptyPasswords no	Denies access to accounts without passwords. Set this 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 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. Set this for all SSH methods of authenticating.
	AllowUsers <i>username</i>	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.

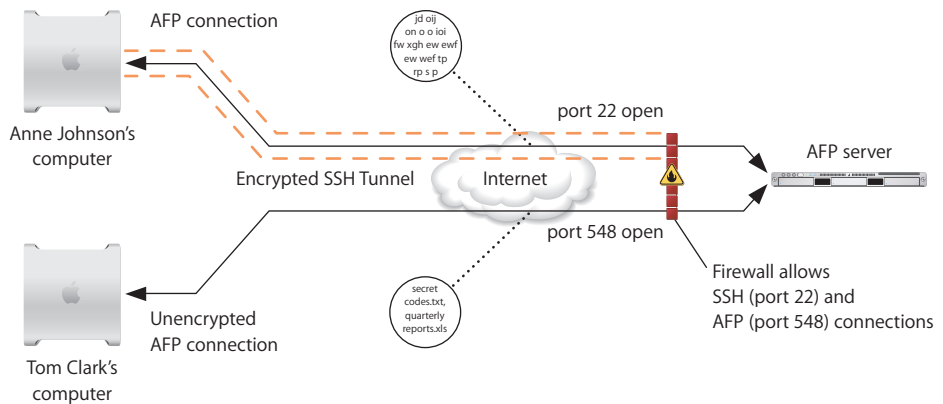
## Using SSH as a Secure Tunnel

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 to log in to the server. A private key is much harder to guess than a password. However, if the home folder where the private key is stored is compromised—assuming the private key is not protected by a password—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.

```
$ ssh-keygen -t dsa
```

- 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 to save the key in (/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, 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 Snow Leopard 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 *Open Directory Administrator*.

## 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 Snow Leopard 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

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. Limit the user’s privileges to the user’s permission on the computer. For example, don’t give a standard user the ability to change 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)
# -----
# Default Setting:
# Remote Management: Disabled

# Suggested Setting:
# Disable Remote Management.
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
    Resources/kickstart -deactivate -stop

# Available Settings:
# Remote Management:
# Disabled
# Enabled
```

## 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.



By default, RAE is turned off and should remain off when it is not used. This prevents unauthorized users from accessing your computer.

From the command line:

```
# Remote Apple Events (RAE)
# -----
# Default Setting:
# Remote Apple Events: Disabled

# Suggested Setting:
# Disable Remote Apple Events.
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.eppc.plist

# Available Settings:
# Remote Apple Events:
# Disabled
# Enabled
```

## 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*.

By default, Xgrid Sharing is turned off and should remain off when it is not 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
# -----
# Default Setting:
# Xgrid Sharing: Disabled

# Suggested Setting:
# Disable Xgrid Sharing.
sudo launchctl unload -w /System/Library/Daemons/com.apple.xgridagentd
sudo launchctl unload -w /System/Library/Daemons/com.apple.xgridcontrollerd

# Available Settings:
# Xgrid Sharing:
# Disabled
# Enabled
```

## 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.

By default, Internet Sharing is turned off and should remain off when it is not used. This prevents unauthorized users from accessing your computer.

From the command line:

```
# Internet Sharing
# -----
# Default Setting:
# Internet Sharing: Disabled

# Suggested Setting:
# Disable Internet Sharing.
sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.nat
    NAT -dict Enabled -int 0
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.InternetSharing.plist

# Available Settings:
# Internet Sharing:
# Disabled
# Enabled
```

## Restricting Access to Specific Users

If 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.

By default, Bluetooth Sharing is turned off and should remain off when it is not 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.

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
# -----
# Default Setting:
# Bluetooth Sharing: Disabled

# Suggested Setting:
# Disable Bluetooth Sharing.
sudo defaults -currentHost write com.apple.bluetooth PrefKeyServicesEnabled
0

# Available Settings:
# Bluetooth Sharing:
# Disabled
# Enabled
```

## Understanding and Managing Daemons and Agents

Daemons and agents, also known as background programs, are programs that run without any graphical user interface. Many of these programs provide important system services that are critical to system functionality.

Snow Leopard uses a process called `launchd` to manage daemons and agents. The `launchd` process is responsible for loading and unloading daemons and agents, and it manages communication between them and the applications or devices they provide services to. You can use the `launchctl` command line program to instruct `launchd` on how to control daemons and agents.

### Listing Active Daemons and Agents on the System

The `launchctl` command can list the daemons and agents available on the system. Many of these daemons and agents provide important services that are critical to system functionality.

Daemons are programs that run in the background as part of the overall system (that is, they are not tied to a particular user). To see a list of the daemons managed by `launchd`, run the following command:

```
$ sudo launchctl list
```

Agents are programs that run in the background on behalf of a user, to provide services to that user. To see a list of the agents managed by `launchd` for you (since you are the current user), run the following command:

```
$ launchctl list
```

In the lists generated by the commands above, the first column shows a process ID number if the daemon or agent is running when the `launchctl` command is run, or it shows a hyphen (-). A major feature of `launchd` is its ability to run daemons or agents only when their services are necessary, in response to a direct need for their services. Daemons and agents that are not running can be activated by `launchd` as needed.

### Configuration Files for Daemons and Agents

Configuration files in the plist format describe how `launchd` controls daemons and agents on the system.

The following table lists the folders where `launchd` reads these configuration files, and the type of configuration file found in each folder.

Folder	Type of Configuration File
~/Library/LaunchAgents	Per-user agents provided by the user
/Library/LaunchAgents	Per-user agents provided by the administrator
/Library/LaunchDaemons	System-wide daemons provided by the administrator

Folder	Type of Configuration File
/System/Library/LaunchAgents	Mac OS X per-user agents
/System/Library/LaunchDaemons	Mac OS X system-wide daemons

## Disabling and Re-enabling Daemons and Agents

Many daemons and agents provide important services that are critical to system functionality. However, in some environments, disabling daemons and agents can be appropriate because their functionality is unneeded or unwanted in that environment. Some of these instances are noted below.

If a daemon or agent must to be disabled, use the `launchctl` command as follows:

```
$ sudo launchctl unload -w <PathToPlist>
```

For example, to disable the daemon that provides Bluetooth service, use the following command:

```
$ sudo launchctl unload -w /System/Library/LaunchDaemons/
    com.apple.blued.plist
```

The `sudo` command is not needed when disabling an agent for the current user.

Disabling daemons or agents creates files in `/var/db/launchd.db` that record which daemons or agents have been disabled. For daemons, the file `/var/db/launchd.db/com.apple.launchd/overrides.plist` is created. For agents, individual folders are created whose names reflect the user id of the user for whom the agent has been disabled.

A user's id number can be found using the `id` program. For example, the user with id 501 stores an `overrides.plist` file in `/var/db/launchd.db/com.apple.launchd.peruser.501/overrides.plist`. These `overrides.plist` files make it easy to identify daemons or agents that are disabled so they can be reenabled later if necessary.

## From the command line:

```
# Understanding and Managing Daemons and Agents
# -----
# Default Setting:
# Airport services: off
# Remote control service: off
# Screen Sharing service: off
# Remote management service: off
# Bluetooth Sharing: off

# Suggested Setting:
# Turn off AirPort Services using the following commands. Run the last
# command as the current user.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.airportPrefsUpdater.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.AirPort.wps.plist
launchctl unload -w /System/Library/LaunchAgents/com.apple.airportd.plist
# Turn off remote control service using the following command:
launchctl unload -w /System/Library/LaunchAgents/com.apple.RemoteUI
# Turn off Screen Sharing services.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.RFBEventHelper.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.RFBRegisterMDNS_RemoteManagement.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.RFBRegisterMDNS_ScreenSharing.plist
launchctl unload -w /System/Library/LaunchAgents/\
com.apple.ScreenSharing.plist
# Turn off Remote Management service using the following commands:
sudo launchctl unload -w /System/Library/LaunchAgents/\
com.apple.RemoteDesktop.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.RemoteDesktop.PrivilegeProxy.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.RFBEventHelper.plist
# Turn off Bluetooth service using the following command:
sudo launchctl unload -w /System/Library/LaunchDaemons/\
com.apple.blued.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)
```

## Where to Get Additional Information

The following resources provide further information about managing daemons and agents:

- *Getting Started with launchd* <http://developer.apple.com/macosx/launchd.html>
- *Introduction to System Startup Programming Topics* <http://developer.apple.com/mac/library/documentation/MacOSX/Conceptual/BPSystemStartup/BPSystemStartup.html>
- Technical Note TN2083 Daemons and Agents <http://developer.apple.com/mac/library/technotes/tn2005/tn2083.html>
- The man pages for launchctl, launchd, and launchd.plist



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 Snow Leopard 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. Changing the region code after it is 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 can 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 Snow Leopard 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 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 Snow Leopard 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 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 credential by consulting the policy database and requesting user authentication.

## Example of Authorizing for Screen Saver

After you configure 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>
  </dict>
  <key>system.login.tty</key>

```

## 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

The verifying of file permissions is a form of file integrity checking. You can use the `pkgutil` command to verify file permissions. For more information about `pkgutil`, see its man page.

Validating a file's integrity is also important because 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.

To prevent this, compare 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.

Snow Leopard 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 40.

## 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 a 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 sealed components are unaltered, and that the 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
```

If all codes verify properly as requested, `codesign` exits. 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.

## Using 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 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 125.

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

Files before rotation	Files after first rotation	File after second rotation
		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. These tools are installed by default. 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/). The mechanism for starting the auditing daemon has changed, but the tools themselves have not.

## Security Auditing

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. Features of the daemon are controlled by the audit utility and the `audit_control` file.

## Enabling Security Auditing

By default, Auditing is turned on in Snow Leopard, but if it is off, you can reenable it using the `launchctl` command.

**To turn auditing on:**

- 1 Open Terminal
- 2 Enter the following command:

```
$ sudo launchctl load -w /System/Library/LaunchDaemons/  
com.apple.auditd.plist
```

## 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 22, 2004 at 18:31:33 and was terminated on March 22, 2004 at 18:44:43.

The audit subsystem appends records to only one audit log file at a time. The 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.

Audit log files are not stored in a human readable format. Use the `praudit` command to print audit records in a human readable form.

By using `praudit -l` option, each record prints on its own line. For example:

```
praudit -l /var/audit/20040322183133.20040322184443
```

For more information about other options, see the `praudit` man page.

The `auditreduce` command provides the ability to search audit records for specific events, users, or times. The following command selects records associated with the effective user root:

```
auditreduce -e root /var/audit/20040322183133.20040322184443
```

For more examples and information, see the `auditreduce` man page.

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 specified folders 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 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).

## Auditing Additional Events

By default, the auditing daemon is configured to watch for login and logout events, authentication and authorization events, and system calls, but other auditable events are possible. You can configure `auditd` to track many more events, and it can be set to do so on a per user basis.

The full list of possible audit event classes can be found in `/etc/security/audit_class` and the full list of events and their mappings to system calls and other actions can be found in `/etc/security/audit_event`. For more information, see the man pages for `audit_control` and `audit_event`.

**To add additional events for all users:**

- 1 Open Terminal.
- 2 Enter the following command to edit the audit control file.

```
$ sudo pico /etc/security/audit_control
```

- 3 Locate the line that begins with “flags” and add auditable events as a comma-delimited list, using the abbreviations found in the `audit_events` file.
- 4 Save the file.

To add events for a user, edit `/etc/security/audit_user` instead and use the following format:

```
username:eventclass1,eventclass2
```

By default, `audit_user` contains an example for the root user.

## Using 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 “Setting Mail Security” on page 165.

When you use antivirus tools, make sure you have the latest virus definition files. The protection provided by 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).

## Using 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.

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.”

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 and set NTP time server		



Action Item	Completed?	Notes
Turn off Auto-login		
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, “Securing System Hardware.”

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.”

Action Items	Completed?	Notes
Require an EFI password		
Create an access warning for the login window		
Create an access warning for the command line		

## System Preferences Action Items

For details, see Chapter 5, “Securing System Preferences.”

Action Items	Completed?	Notes
Log in with administrator privileges		
Enable MobileMe 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 Keyboard preferences		
Securely configure Mouse preferences		
Securely configure Print & Fax preferences		
Securely configure Network preferences		
Securely configure Parental Control 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		

## Account Configuration Action Items

For details, see Chapter 6, “Securing Accounts.”

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 sudo 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		

Action Item	Completed?	Notes
Secure keychain items		
Create keychains for specialized purposes		
Use a portable drive to store keychains		

## Encryption (DAR) Action Items

For details, see Chapter 7, “Securing Data and Using Encryption.”

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		

## Application Action Items

For details, see Chapter 8, “Securing Applications.”

Action Items	Completed?	Notes
Configure Mail using SSL		
Disable the Preview Pane for Mail Messages		
Disable Auto-Fill		
Block Pop-ups		
Only Allow Cookies from Visited Sites		
Disable opening safe files in Safari		
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 9, “Securing Network Services.”

Action Items	Completed?	Notes
Configure IPFW2 firewall		
Implement IPFW ruleset		
Enable firewall logging		
Implement inclusive ruleset		
Set ruleset to permit services		
Set more restrictive ruleset		
Configuring System to load IPFW ruleset		
Bonjour		
Secure BTMM access through Security Preferences		
Set up screen sharing through VNC with password protection		
Disable Screen Sharing when possible		
Disable File Sharing when possible		
Disable Printer Sharing when possible		
Disable Scanner Sharing when possible		
Disable Web Sharing when possible		
Disable Remote Login when possible		
Establish key-based SSH connections		
Configure ARD to manage remote tasks		
Disable Remote Management when possible		
Disable Remote Apple Events when possible		
Disable Xgrid Sharing when possible		

Action Items	Completed?	Notes
Disable Internet Sharing when possible		
Disable Bluetooth Sharing when possible		

### Advanced Management Action Items

For details, see Chapter 10, “Advanced Security Management.”

Action Item	Completed?	Notes
Create an authorization right to the dictionary to authorize users		
Create a digital signature		
Enable security auditing		
Configure security auditing		
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
# -----
# Default Settings:
# blank
# Software updates are downloaded from one of the following software update
# servers hosted by Apple:
# swscan.apple.com:80
# swquery.apple.com:80
# swcdn.apple.com:80

# Suggested Settings:
# Specify the software update server to use.
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL
    http://swupdate.apple.com:8088/index-leopard-snowleopard.merged-
    1.sucatalog

# Available Settings:
# Replace swupdate.apple.com with the fully qualified domain name (FQDN)
# or IP address of your software update server.

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

# Updating from Internet Software Update Server
# -----
# Default Settings:
# The softwareupdate command by default checks and lists available
# updates for download. Software Update preferences are set to the
# command-line equivalent of:
# softwareupdate --list --schedule on

# Suggested Settings:
# Download and install software updates.
sudo softwareupdate --download --all --install
```

```

# Available Settings:
# Use the following commands to view softwareupdate options:
# $ softwareupdate -h
# or
# $ man softwareupdate

# Updating Manually from Installer Packages
# -----
# Default Settings:
# None

# Suggested Settings:
# Download software updates.
sudo softwareupdate --download --all
# Install software updates.
sudo installer -pkg $Package_Path -target /Volumes/$Target_Volume

# Available Settings:
# Use the following commands to view installer options:
# $ installer -h
# or
# $ man installer

# Verifying the Integrity of Software
# -----
# Default Settings:
# None

# Suggested Settings:
# 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.
sudo /usr/bin/openssl sha1 $full_path_filename

# Available Settings:
# Use the following command to view the version of OpenSSL installed on
# your computer:
# $ openssl version
# Use the following command to view openssl options:
# $ man openssl

```



```

# Using Disk Utility to Repair Disk Permissions
# -----
# Default Setting:
# None

# Suggested Setting:
# Verify disk permissions
sudo diskutil verify Permissions /Volumes/$Target_Boot_Drive
# If permission discrepancies exist that were not set by your
# organizations, use the following Repair disk permissions command:
sudo diskutil repairPermissions /Volumes/$Target_Boot_Drive

# Available Setting:
# Use the following command to view diskutil options:
# $ diskutil

# -----
# Securing System Hardware
# -----
# Removing Wi-Fi Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Apple AirPort kernel extensions.
sudo srm -rf /System/Library/Extensions/IO80211Family.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
# Removing BlueTooth Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Bluetooth kernel extensions.
sudo srm -rf /System/Library/Extensions/IOBluetoothFamily.kext
sudo srm -rf /System/Library/Extensions/IOBluetoothHIDDriver.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None

```

```

# Removing IR Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove IR kernel extensions.
sudo srm -rf /System/Library/Extensions/AppleIRController.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None

# Securing Audio Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Audio Recording kernel extensions.
sudo srm -rf /System/Library/Extensions/AppleUSBAudio.kext
sudo srm -rf /System/Library/Extensions/IOAudioFamily.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None

# Securing Video Recording Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove Video Recording kernel extensions.
# Remove external iSight camera.
sudo srm -rf /System/Library/Extensions/Apple_iSight.kext
# Remove internal iSight camera.
sudo srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/PlugIns/\
    AppleUSBVideoSupport.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None

```

```

# Securing USB Support Software
# -----
# Remove USB kernel extensions.
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
sudo srm -rf /System/Library/Extensions/IOUSBMassStorageClass.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None
# Securing FireWire Support Software
# -----
# Default setting:
# kext files are installed and loaded.

# Suggested Setting:
# Remove FireWire kernel extensions.
sudo srm -rf /System/Library/Extensions/\
    IOFireWireSerialBusProtocolTransport.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings:
# None

# Securing Global System Settings
# -----
# Configuring EFI Settings
# -----
# Default Setting:
# security-mode is off

# Suggested Setting:
# Secure startup by setting security-mode. Replace $mode-value with
# "command" or "full."
sudo nvram security-mode="$mode-value"
# Verify security-mode setting.
sudo nvram -x -p

```

```

# Available Settings:
# security-mode:
# "command"
# "full"
# Use the following command to view the current nvram settings:
# $ nvram -x -p
# Use the following commands to view nvram options:
# $ nvram -h
# or
# $ man nvram

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

# Enabling Access Warning for the Command Line
# -----
# Create a command-line access warning.
sudo touch /etc/motd
sudo chmod 644 /etc/motd
sudo echo "Warning Text" >> /etc/motd

# -----
# Securing System Preferences
# -----
# Securing MobileMe Preferences
# -----
# Default Setting:
# If a MobileMe account is entered during setup, MobileMe is configured
# for that account.
# Use the following command to display current MobileMe settings:
# $ defaults -currentHost read com.apple.<Preferenceidentifier>
# Use the following command to view all current settings for currenHost:
# $ defaults -currentHost read

# Suggested Setting:
#Disable Sync options.
sudo defaults -currentHost write com.apple.DotMacSync ShouldSyncWithServer 1
# Disable iDisk Syncing.
sudo defaults -currentHost write com.apple.idisk $USER_MirrorEnabled -bool
    no

# Available Settings:
# None

```

```

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

# Securing Appearance Preferences
# -----
# Default Setting:
# MaxAmount 10

# Suggested Setting:
# Disable display of recent applications.
sudo defaults write com.apple.recentitems Applications -dict MaxAmount 0

# Available Settings:
# MaxAmount 0,5,10,15,20,30,50

# Securing Bluetooth Preferences
# -----
# Default Setting:
# Turn Bluetooth on.

# Suggested Setting:
# Turn Bluetooth off.
sudo defaults write /Library/Preferences/com.apple.Bluetooth\
    ControllerPowerState -int 0

# Available Settings:
# 0 (OFF) or 1 (On)

```

```

# Securing CDs & DVDs Preferences
# -----
# Default Setting:
# Preference file non existent: /Library/Preferences/com.apple.digihub
# Blank CD: "Ask what to do"
# Blank DVD: "Ask what to do"
# Music CD: "Open iTunes"
# Picture CD: "Open iPhoto"
# Video DVD: "Open DVD Player"

# Suggested Setting:
# Disable blank CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.cd.appeared -dict action 1
# Disable music CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.music.appeared -dict action 1
# Disable picture CD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.cd.picture.appeared -dict action 1
# Disable blank DVD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.blank.dvd.appeared -dict action 1
# Disable video DVD automatic action.
sudo defaults write /Library/Preferences/com.apple.digihub
    com.apple.digihub.dvd.video.appeared -dict action 1

# Available Settings:
# action 1 = "Ignore"
# action 2 = "Ask what to do"
# action 5 = "Open other application"
# action 6 = "Run script"
# action 100 = "Open Finder"
# action 101 = "Open iTunes"
# action 102 = "Open Disk Utility"
# action 105 = "Open DVD Player"
# action 106 = "Open iDVD"
# action 107 = "Open iPhoto"
# action 109 = "Open Front Row"

```

```

# Securing Date & Time Preferences
# -----
# Default Setting:
# NTP Server: time.apple.com
# Time Zone: Set time zone automatically using current location

# Suggested Setting:
# Set the NTP server.
sudo cat >> /etc/ntp.conf << END server time.apple.com END
# Set the date and time.
sudo systemsetup -settimezone $Time_Zone

# Available Settings:
# NTP Server: Any valid NTP server
# Time Zone: /usr/share/zoneinfo

# Securing Desktop & Screen Saver Preferences
# -----
# Default Setting:
# None

# Suggested Setting:
# Set idle time for screen saver. Replace XX with the idle time in seconds.
sudo defaults -currentHost write com.apple.screensaver idleTime -int XX
# Set host corner to activate screen saver.
sudo defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
corner -int 5
# Set modifier key to 0 wvous-corner_code-modifier
sudo defaults write /Library/Preferences/com.apple.dock.wvous-corner_code-
modifier -int 0

# Available Settings:
# Corner options:
# wvous-bl-corner (bottom-left)
# wvous-br-corner (bottom-right)
# wvous-tl-corner (top-left)
# wvous-tr-corner (top-right)

```

```

# Securing Dock Preferences
# -----
# Default Setting:
# None

# Suggested Setting:
# Automatically hide and show Dock.
sudo defaults write /Library/Preferences/com.apple.dock autohide -bool YES

# Available Settings:
# autohide -bool YES
# autohide -bool NO

# Securing Energy Saver Preferences
# -----
# Default Setting:
# None

# Suggested Setting:
# Disable computer sleep.
sudo pmset -a sleep 0
# Enable hard disk sleep.
sudo pmset -a disksleep 1
# Disable Wake for Ethernet network administrator access.
sudo pmset -a womp 0
# Disable Restart automatically after power failure.
sudo pmset -a autorestart 0

# Available Settings:
# 0 (OFF) or 1 (ON)

# Securing Exposé & Spaces Preferences
# -----
# Default Setting:
# Enabled

# Suggested Setting:
# Disable dashboard.
sudo launchctl unload -w /System/Library/LaunchDaemons/
    com.apple.dashboard.advisory.fetch.plist

# Available Settings:
# Enabled or Disabled

```



```

# Securing Network Preferences
# -----
# Default Setting:
# Enabled

# Suggested Setting:
# Disable IPv6.
sudo networksetup -setv6off $interface

# Available Settings:
# The interface value can be AirPort, Bluetooth, Ethernet, or FireWire.

# Securing Print & Fax Preferences
# -----
# Default Setting:
# Disabled

# Suggested Setting:
# Disable the receiving of faxes.
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.efax.plist
# Disable printer sharing.
sudo 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

# Available Settings:
# Enabled or Disabled

# Securing Security Preferences
# -----
# Default Setting:
# Required Password Wake: Disabled
# Automatic Login: Disabled
# Password Unlock Preferences: Disabled
# Secure Virtual Memory is Enabled on Portable computer and is Disabled
# on Desktop computers.
# IR remote control: Enabled
# FileVault: Disabled

```

```

# Suggested Setting:
# Enable Require password to wake this computer from sleep or screen saver.
sudo defaults -currentHost write com.apple.screensaver askForPassword -int 1
# Disable Automatic login.
sudo defaults write /Library/Preferences/.GlobalPreferences\
com.apple.userspref.DisableAutoLogin -bool yes
# Require 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.
sudo defaults write /Library/Preferences/.GlobalPreferences\
com.apple.autologout.AutoLogOutDelay -int 0
# Enable secure virtual memory.
sudo defaults write /Library/Preferences/com.apple.virtualMemory\
    UseEncryptedSwap -bool yes
# Disable IR remote control.
sudo defaults write /Library/Preferences/com.apple.driver.AppleIRController
    DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
sudo /System/Library/CoreServices/ManagedClient.app/Contents/Resources/\
createmobileaccount
# Enable Firewall.
# Replace value with
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
sudo defaults write /Library/Preferences/com.apple.alf globalstate -int
    value
# Enable Stealth mode.
sudo defaults write /Library/Preferences/com.apple.alf stealthenabled 1
# Enable Firewall Logging.
sudo defaults write /Library/Preferences/com.apple.alf loggingenabled 1

# Securing System Swap and Hibernation Storage
# -----
# Default Setting:
# Secure Virtual Memory on Portable computers is Enabled and is Disabled on
# Desktop computers.

# Suggested Setting:
# Enable secure virtual memory.
sudo defaults write /Library/Preferences/com.apple.virtualMemory\
    UseEncryptedSwap -bool YES

```

```

# Available Setting:
# UseEncryptedSwap -bool NO
# UseEncryptedSwap -bool YES
# You can also turn hibernate off by using the following command:
# sudo pmset hibernatemode 0

# Securing Sharing Preferences
# -----
# Default Setting:
# $host_name = User's Computer

# Suggested Setting:
# Change computer name where $host_name is the name of the computer.
sudo systemsetup -setcomputername $host_name
# Change computer Bonjour host name.
sudo scutil --set LocalHostName $host_name

# Available Setting:
# The host name cannot contain spaces or other non-DNS characters.
# Securing Software Updates Preferences
# -----
# Default Setting:
# Check for Updates: Enabled
# Check Updates: Weekly

# Suggested Setting:
# Disable check for updates and Download important updates automatically.
sudo softwareupdate --schedule off

# Available Setting:
# Check for Updates: Enabled or Disabled
# Check Updates: Daily, Weekly, Monthly

# Securing Sound Preferences
# -----
# Default Setting:
# Internal microphone or line-in: Enabled

# Suggested Setting:
# Disable internal microphone or line-in.
# This command does not change the input volume for input devices. It
# only sets the default input device volume to zero.
sudo osascript -e "set volume input volume 0"

# Available Setting:
# Internal microphone or line-in: Enabled or Disabled

```

```

# Securing Speech Preferences
# -----
# Default Setting:
# Speech Recognition: Disabled
# Text to Speech: Enabled

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

# Available Setting:
# Each item can be set to ON or OFF:
# OFF: -bool false
# ON: -bool true

# Securing Spotlight Preferences
# -----
# Default Setting:
# ON for all volumes

# Suggested Setting:
# Disable Spotlight for a volume and erase its current meta data, where
# $volumename is the name of the volume.
sudo mdutil -E -i off $volumename

# Available Setting:
# Spotlight can be turned ON or OFF for each volume.

# Securing Startup Disk Preferences
# -----
# Default Setting:
# Startup Disk = "Macintosh HD"

# Suggested Setting:
# Set startup disk.
sudo systemsetup -setstartupdisk $path

```

```

# Available Setting:
# Startup Disk = Valid Boot Volume

# Securing Time Machine Preferences
# -----
# Default Setting:
# OFF

# Suggested Setting:
# Enable Time Machine.
sudo defaults write /Library/Preferences/com.apple.TimeMachine AutoBackup 1

# Available Setting:
# 0 (OFF) or 1 (ON)

# Securing Universal Access Preferences
# -----
# Default Setting:
# OFF

# Suggested Setting:
# Disable VoiceOver service.
launchctl unload -w /System/Library/LaunchAgents/com.apple.VoiceOver.plist
launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.ScreenReaderUIServer.plist
launchctl unload -w /System/Library/LaunchAgents/com.apple.scrod.plist

# Available Setting:
# None

# -----
# Securing Applications
# -----
# Disabling iSync
# -----
# Default Setting:
# OFF

# Suggested Setting:
# Disable iSync.
launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.syncservices.SyncServer.plist
launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.syncservices.uihandler.plist

# Available Setting:
# None

```

```

# -----
# Securing Network Services
# -----
# Disabling IKE VPN Key Management Service
# -----
# Default Setting:
# OFF

# Suggested Setting:
# If a VPN is not used, disable the IKE VPN key management service.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.racoon.plist

# Available Setting:
# None

# Block Bonjour listening
# -----
# Default Setting:
# Bonjour is enabled.
# Firewall is disabled.

# Suggested Setting:
# Reload the firewall rules.
sudo /sbin/ipfw flush

# Available Settings:
# Disable firewall and allow Bonjour.
# Enable firewall and block port 5353.

# Enable Bonjour Service
# -----
# Default Setting:
# Bonjour is enabled
# Firewall is disabled

# Suggested Setting:
# Remove the following line from /etc/ipfw.conf.
add 00001 deny udp from any to me dst-port 5353
# Reload the firewall rules
sudo /sbin/ipfw flush

# Available Settings:
# Disable Firewall and allow Bonjour
# Enable Firewall and block port 5353

```

```

# DVD or CD Sharing
# -----
# Default Setting:
# Disabled (unload)

# Suggested Setting:
# Disable DVD or CD Sharing.
sudo launchctl unload -w /System/Library/LaunchDaemons\
    com.apple.ODSAgent.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)

# Screen Sharing (VNC)
# -----
# Default Setting:
# Disabled

# Suggested Setting:
# Disable Screen Sharing.
sudo srm /private/etc/ScreenSharing.launchd

# Available Settings:
# Enabled:
# "All Users"
# "Only these users"

# Disable File Sharing services.
# -----
# Default Setting:
# File Sharing Disabled:
# AFP
# FTP
# SMB
# NFS

```

```

# Suggested Setting:
# Disable FTP.
sudo launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
# Disable SMB.
sudo defaults delete /Library/Preferences/SystemConfiguration/\
    com.apple.smb.server EnabledServices
sudo launchctl unload -w /System/Library/LaunchDaemons/nmbd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/smbd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smb.server.preferences.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smb.sharepoints.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.smbfs_load_kext.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    org.samba.winbindd.plist
# Disable AFP.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.AppleFileServer.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.afpfs_afpLoad.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.afpfs_checkafp.plist
# Disable NFS
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.nfsd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.lockd.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.statd.notify.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.portmap.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)

# Web Sharing
# -----
# Default Setting:
# Web Services: Disabled

# Suggested Setting:
# Disable Web Sharing.
sudo launchctl unload -w /System/Library/LaunchDaemons/
    org.apache.httpd.plist

```



```

# Available Settings:
# Web Services:
# Disabled
# Enabled

# Remote Login (SSH)
# -----
# Default Setting:
# Remote Login (SSH): Disabled

# Suggested Setting:
# Disable Remote Login.
sudo launchctl unload -w /System/Library/LaunchDaemons/ssh.plist

# Available Settings:
# Remote Login (SSH):
# Disabled
# Enabled

# Remote Management (ARD)
# -----
# Default Setting:
# Remote Management: Disabled

# Suggested Setting:
# Disable Remote Management.
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
    Resources/kickstart -deactivate -stop

# Available Settings:
# Remote Management:
# Disabled
# Enabled

# Remote Apple Events (RAE)
# -----
# Default Setting:
# Remote Apple Events: Disabled

# Suggested Setting:
# Disable Remote Apple Events.
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.eppc.plist

```

```

# Available Settings:
# Remote Apple Events:
# Disabled
# Enabled

# Xgrid Sharing
# -----
# Default Setting:
# Xgrid Sharing: Disabled

# Suggested Setting:
# Disable Xgrid Sharing.
sudo launchctl unload -w /System/Library/Daemons/com.apple.xgridagentd
sudo launchctl unload -w /System/Library/Daemons/com.apple.xgridcontrollerd

# Available Settings:
# Xgrid Sharing:
# Disabled
# Enabled

# Internet Sharing
# -----
# Default Setting:
# Internet Sharing: Disabled

# Suggested Setting:
# Disable Internet Sharing.
sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.nat
    NAT -dict Enabled -int 0
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.InternetSharing.plist

# Available Settings:
# Internet Sharing:
# Disabled
# Enabled

# Bluetooth Sharing
# -----
# Default Setting:
# Bluetooth Sharing: Disabled

# Suggested Setting:
# Disable Bluetooth Sharing.
sudo defaults -currentHost write com.apple.bluetooth PrefKeyServicesEnabled
    0

```

```

# Available Settings:
# Bluetooth Sharing:
# Disabled
# Enabled

# Understanding and Managing Daemons and Agents
# -----
# Default Setting:
# Bluetooth Sharing: off

# Suggested Setting:
# Turn off AirPort Services using the following commands. Run the last
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.airportPrefsUpdater.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.AirPort.wps.plist
launchctl unload -w /System/Library/LaunchAgents/com.apple.airportd.plist
# Turn off remote control service using the following command:
launchctl unload -w /System/Library/LaunchAgents/com.apple.RemoteUI
# Turn off Screen Sharing services.
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.RFBEventHelper.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.RFBRegisterMDNS_RemoteManagement.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.RFBRegisterMDNS_ScreenSharing.plist
launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.ScreenSharing.plist
# Turn off Remote Management service using the following commands:
sudo launchctl unload -w /System/Library/LaunchAgents/\
    com.apple.RemoteDesktop.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.RemoteDesktop.PrivilegeProxy.plist
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.RFBEventHelper.plist
# Turn off Bluetooth service using the following command:
sudo launchctl unload -w /System/Library/LaunchDaemons/\
    com.apple.blued.plist

# Available Settings:
# Disabled (unload)
# Enabled (load)

```

# Index

## A

access control entries. *See* ACEs  
 access rights. *See* permissions  
 access warnings 57–60  
     *See also* permissions  
 accounts  
     administrator 33–34, 118–119, 124–127  
     authentication setup 62, 130  
     checklists 243–244  
     creating secure 121–127  
     credential storage 134–139  
     directory domains 127–129  
     initial setup 34  
     mobile 127  
     nonadministrator user 118–119  
     preferences 67–69  
     types 118  
 ACEs (access control entries) 41, 147  
 ACLs (access control lists) 41, 135, 143, 147–148, 163  
 Active Directory 129  
 activity analysis tools 233–236  
 Address Book 128, 181  
 administrator account 33–34, 118–119, 124–127  
 Advanced Encryption Standard (AES-128) 99  
 AFP (Apple Filing Protocol) 201–202  
 antivirus tools. *See* virus screening  
 appearance preferences 70–71  
 Apple Filing Protocol. *See* AFP  
 Apple Remote Desktop. *See* ARD  
 Apple Software Restore. *See* ASR  
 Application firewall 184–186  
 applications  
     access control 23, 24, 186  
     securing 165–170, 232–233  
 ARD (Apple Remote Desktop) 215–216  
 ASR (Apple Software Restore) 33  
 assistive devices 117  
 attributes, rules 227  
 auditing tools 236–238  
 authentication  
     accurate time settings 35  
     Active Directory 129  
     Directory Access 128–129

key-based SSH 213–215  
     *See also* keychain services; passwords  
     server- vs. client-side 170  
     strengthening methods 130–133  
     system preferences 63  
     user  
 authorization 225  
     *See also* authentication  
 authorization rights 228–230  
 AutoFill options 170, 175  
 automatic actions, disabling 73

## B

Back to My Mac. *See* BTMM  
 backups 163–164  
 BannerSample file, modifying 59  
 Berkeley Software Distribution. *See* BSD  
 Bill of Materials file 41  
 biometrics-based authentication 133  
 Bluetooth preferences 72–73, 220  
 Bonjour browsing service 194  
 bookmarks, synchronizing 174  
 Boot Camp 163  
 browsers  
     preferences 174  
     security 170  
 BSD (Berkeley Software Distribution) 18, 234  
 BTMM (Back to My Mac) 197–198

## C

CA. *See* Certificate Authority  
 cache, browser 170  
 CDs, preferences 73, 199  
 CDSA (Common Data Security Architecture) 18  
 CERT (Computer Emergency Response Team) 18  
 Certificate Assistant 171–172  
 Certificate Authority 171–172  
 Certificate Revocation List. *See* CRL  
 certificates 21, 27, 155, 165–169, 178–180  
**checksum** tool 231  
 CIFS (Common Internet File System). *See* SMB  
 Click 93  
 client-side authentication 170

- codesign command 233
- command-line interface
  - access warnings 60
  - erasing files 161
  - ssh access 205–215
  - startup security setup 56
- command-line tools, Firewall service 187
- Common Criteria Tools 236
- Common Data Security Architecture. *See* CDSA
- Common Security Service Manager. *See* CSSM
- Computer Emergency Response Team. *See* CERT
- computers, host name 106
- configuration files 212
- Console tool 234
- contacts search policy 128–129
- cookies 170, 177
- credential storage 134–139
- CRL (Certificate Revocation List) 171
- CSSM (Common Security Service Manager) 21

## D

- Dashboard preferences 83–84
- data security 104, 143–162, 163–164
- Date & Time preferences 75–76
- Desktop preferences 77–78
- dictionaries
  - rights 225–227
  - rules 227
- digital signature 165–169, 232–233
- directories. *See* directory services; domains, directory; folders
- Directory Access 128–129
- directory services
  - Active Directory 129
  - directory domains 127–129
  - Open Directory 129
- discovery, service 128
- disk images
  - encrypting 28, 157–159, 182
  - read/write 157
  - restoring from 33
- disks
  - permissions for 40–42
  - startup 114–115
- Disk Utility 28, 41, 160, 162
- display mirroring 79
- Displays preferences 79
- Dock preferences 79
- domains, directory 127–129
- Download Inspector 25
- DVDs, preferences 73, 199

## E

- EFI (Extensible Firmware Interface) 54, 115
- email. *See* Mail service

- Enabling 60
- encryption
  - disk images 157–159
  - FileVault 29, 153–156
  - Mail service 165–169
  - secure virtual memory 104
  - Time Machine 163–164
- Energy Saver preferences 80–81
- erasing data permanently 159–162
- Everyone permission level 144
- Exposé & Spaces preferences 83–84
- Extensible Firmware Interface. *See* EFI

## F

- fax preferences 96–98
- files
  - backup of 163–164
  - Bill of Materials 41
  - downloading safely 173
  - encryption 153–159
  - erasing 159–162
  - integrity checking tools 232
  - managing log 234
  - package 41
  - permissions 143–146, 148–149
  - security 104, 177
- file services
  - See also* FTP; share points
- file sharing 201–202
- file systems, erasing data 159
- File Transfer Protocol. *See* FTP
- FileVault 29, 43, 99, 153–156, 157, 207
- FileVault master keychain 154
- fingerprints, server 206, 214–215
- Firewall service 26, 106, 183–186
- FireWire 114
- FireWire Bridge Chip GUID 114
- Firmware interface 55
- firmware password 55, 114–115
- flags for files and folders 146–147
- folders
  - flags for 146–147
  - home 127, 152–156
  - permissions for 152–153
  - shared 182
- free disk space, erasing 162
- FTP (File Transfer Protocol) 201–202

## G

- global file permissions 148–149
- grids, server 217–218
- groups, permissions 144
- guest accounts, permissions 144
- guest operating systems 163

## H

- hard drive 43
- hardware, protection of 43, 241, 245
- HIDS (host-based intrusion detection systems) 239
- HISEC (Highly Secure) templates 129
- home folders 127, 152–156
- host name 106
- hosts. *See* servers
- HTML (Hypertext Markup Language) email 166

## I

- iChat service 178, 178–180, 181
- iDisk 182
- images. *See* disk images
- installation 31–42, 107, 240–241
- installer packages 107
- Intel-based Macintosh 54, 163
- International preferences 84
- Internet-based Software Update 36
- Internet security
  - browsers 170, 176
  - email 165–169
  - instant messaging 178–180
  - MobileMe preferences 64–66
  - sharing 105–106, 181, 197–198, 217–220
- intrusion detection system (IDS) monitors 239
- IP addresses 85
- IPFW2 software 187
- iPhoto 181
- IPv6 addressing 85
- iTunes 181

## K

- Kerberos 129, 131–132, 165
- key-based SSH connection 207–210, 213–215
- Keyboard preferences 84
- Keychain Access 134, 169, 171–172
- keychain services 21, 23, 134–139, 154

## L

- L2TP/IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) 192–194
- Launch Services 25
- layered security architecture 20
- LDAP (Lightweight Directory Access Protocol) service 129
- LDAPv3 access
- Lightweight Directory Access Protocol. *See* LDAP
- local system logging 235
- locking folders 146
- logging tools 234–236
- login
  - access warnings 57–60
  - automatic 99
  - keychain 135–136

- remote 205–215, 217
- security measures 67–69, 239

## logs

- audit 237–238
- security 234–236

## M

- Mach 18
- Mail service 165–169
- managed preferences
  - Dashboard 83–84
  - Date & Time 75–76
  - Desktop 77–78
  - Displays 79
  - Dock 79
  - Energy Saver 80–81
  - Exposé & Spaces 83–84
  - International 84
  - Keyboard 84
  - MobileMe 64–66
  - Mouse 84
  - Network 85–86, 87
  - Parental Controls 93–95
  - Print & Fax 96–98
  - Security 99–101, 184
  - Sharing 105–106, 184, 206, 216–220
  - Software Update 36–39, 107
  - Sound 109
  - Spotlight 111–113
  - Startup Disk 114–115
  - Time Machine 115–116, 163–164
  - Universal Access 117
- managed user accounts 118
- mandatory access controls 23–25
- Microsoft Windows compatibilities 147
- mobile accounts 127
- MobileMe preferences 64–66, 178–180
- Mouse preferences 84

## N

- NetBoot service 33
- network-based directory domains 127–129
- network-based intrusion detection systems. *See* NIDS
- network-based keychains 139
- network install image 114
- Network preferences 87
- network services
  - access control 87
  - FileVault limitations 153, 157
  - installation 32
  - keychains 139
  - logs 234–236
  - managed users 121
  - preferences 85–86
  - security methods 27, 165, 183–186

- sharing 105–106, 199, 217–220
- sleep mode security 80
- Software Update cautions 36
- wireless preferences 72–73
- `newsyslog` command 236
- NIDS (network-based intrusion detection systems) 239
- nonadministrator user accounts 118–119
- NTP (network time protocol) 35
- `nvr` tool 56

## O

- Open Directory 129
- open source software 18–20
- owner permission 144

## P

- packages, file 41
- Parental Controls 24, 93–95, 121–124
- Password Assistant 68, 130–131
- passwords
  - authentication setup 130–131, 166–167
  - changing 67–69
  - command-line tools 56
  - firmware 55, 114–115
  - keychain 135
  - master FileVault 154–156
  - Startup Disk preferences 114–115
  - tokens 133
  - vs. key-based authentication 207
- PDFs, encrypted 159
- permissions
  - access 18
  - disk 40–42
  - folders 152–153
  - manipulating 146
  - overview 143–149
  - user 202
  - viewing 144
- physical access, securing 43
- physical computers
  - hardware security 44
- PKI (public key infrastructure) 21, 165, 179, 207
  - See also* certificates
- plug-ins 176
- policy database 225–228
- portable computers
  - FileVault 153
  - keychains 139
  - mobile accounts 127
- portable files, encrypting 157–159
- portable keychains 139
- POSIX (Portable Operating System Interface) 41, 144–149
- preferences

- accounts 67–69
- appearance 70–71
- Bluetooth wireless 72–73, 220
- CDs 73, 199
- cookies 177
- DVDs 73, 199
- fax 96–98
- overview 62, 63
- screen saver 77–78
  - See also* managed preferences
- speech recognition 110
- time 75–76
- Print & Fax preferences 96–98
- Printer Sharing 204
- privacy option, iChat service 179
- private browsing 170
- private key 207
- privileges vs. permissions 40
- protocols. *See specific protocols*
- proxy settings 177
- public key cryptography 232–233
- public key infrastructure. *See* PKI
- `wpolicy` command 133

## Q

- Quarantine 25

## R

- read/write disk images 157
- recent items list 70–71
- Remote Apple Events 216
- remote images in email 166
- Remote Login 205–215
- remote server login 217
- remote system logging 236
- removable media
  - FileVault limitations 153, 157
- rights dictionary 225–227
- right specifications 225–227
- root permissions 54, 125–126
- rules dictionary 227

## S

- Safari preferences 170, 173–177
- sandboxing 24
- Scanner Sharing 204
- screen saver preferences 77–78, 99
- Screen Sharing 200
- searching preferences 111–113
- Secure Empty Trash command 162
- Secure iChat certificate 179
- secure notes 134
- Secure Sockets Layer. *See* SSL
- Secure Transport 20
- security 104, 181

- security architecture overview 18–21
- security-mode environment variable 56
- security-password environment variable 56
- Security preferences 99–101, 184
- Server Message Block/Common Internet File System. *See* SMB
- servers
  - authentication 171–172
  - fingerprints 206, 214–215
  - securing connections 210
- server-side authentication 170
- Setup Assistant 33–34
- SHA-1 digest 40
- shared resources
  - printers 96, 98
  - user accounts 119
- share points 201–202
- Sharing preferences 105–106, 184, 206, 216–220
- Simple Finder 122
- single sign-on (SSO) authentication 131–132
  - See also* Kerberos
- single-user mode 54
- sleep mode, securing 80–81, 99
- smart cards 29, 132
- SMB (Server Message block) 201–202
- software, networking 165, 186
- Software Update service 35, 36–39, 107
- Sound preferences 109
- sparse images 157
- speech recognition preferences 110
- Spotlight preferences 111–113
- srm** command 161
- SSH (secure shell host) 205–215
- ssh** command 205–215
- SSL (Secure Sockets Layer) 20, 165, 179
- standard user accounts 118
- startup, securing 54–55
- Startup Disk preferences 114–115
- stealth mode 185
- sudo** tool 125–127
- su** tool 126
- swap file 100
- synchronization 64–66, 174
- syslogd configuration file 235
- system administrator (root) account 125–127
- system preferences. *See* preferences
- system setup 33–35

## T

- target disk mode 115
- third-party applications 83

- ticket-based authentication 129
- Time Machine 115–116, 163–164
- time settings 35, 75–76
- TLS (Transport Layer Security) protocol
- tokens, digital 133
- Transport Layer Security protocol. *See* TLS
- transport services 20
- tunneling protocols
  - SSH 211
  - VPN 192–194
- two-factor authentication 29

## U

- UIDs (user IDs) 119–120
- Universal Access preferences 117
- UNIX and security 18
- updating software 35–39, 107
- user accounts 118–127
- user ID. *See* UID
- users
  - access control 24, 121–124, 202, 228–230
  - automatic actions control 73
  - home folders 127, 152–156
  - keychain management 137–138
  - mobile 127
  - permissions 41, 144
  - preferences control 78, 83
  - root 54
  - See also* user accounts

## V

- validation, system integrity 231–232, 246
- virtual memory 100, 104
- Virtual Network Communication. *See* VNC
- virus screening 239
- VNC (Virtual Network Communication) 200
- volumes, erasing data 159
- VPN (Virtual Private Network)
  - clients 27
  - security 192–194

## W

- web browsers. *See* browsers
- web forms, completing 175
- Web Sharing 204
- websites, sharing 204
- wireless preferences 72–73

## X

- Xgrid 217–218