




Mac OS X

Security Configuration
For Version 10.4 or Later
Second Edition

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

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

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

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

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, FireWire, Keychain, Mac, Macintosh, the Mac logo, Mac OS, QuickTime, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries. Apple Remote Desktop, Finder, and Xgrid are trademarks of Apple Inc.

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

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

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.

019-0922/02-15-07

Contents

Preface	9 About This Guide
	9 Target Audience
	9 What's New in Mac OS X Version 10.4
	10 What's in This Guide
	11 Using This Guide
	11 Using Onscreen Help
	11 Mac Help
	12 The Mac OS X Server Suite
	13 Getting Documentation Updates
	13 Getting Additional Information
	14 Acknowledgments
Chapter 1	15 Introducing Mac OS X Security Architecture
	16 Security Architectural Overview
	16 UNIX Infrastructure
	16 Access Permissions
	16 Security Framework
	17 Layered Security Defense
	18 Built-In Security Services
	18 Keychain Services
	18 Secure Transport Services
	18 Certificate, Key, and Trust Services
	18 Authorization Services
	19 Smart Card Services
	19 Authorization versus Authentication
Chapter 2	21 Installing Mac OS X
	21 System Installation Overview
	21 Disabling the Open Firmware Password
	22 Installing from CD or DVD
	23 Installing from the Network
	23 Restoring from Preconfigured Disk Images
	23 Initializing System Setup

- 23 Using Setup Assistant
- 24 Creating Initial System Accounts
- 25 Setting Correct Time Settings
- 25 Updating System Software
- 26 Updating from an Internal Software Update Server
- 27 Updating from Internet-Based Software Update Servers
- 27 Updating Manually from Installer Packages
- 28 Verifying the Integrity of Software
- 28 Repairing Disk Permissions
- 29 Kinds of Permissions
- 29 POSIX Permissions Overview
- 29 ACL Permissions Overview
- 30 Using Disk Utility to Repair Disk Permissions

Chapter 3

- 31 **Protecting Hardware and Securing Global System Settings**
- 31 Protecting Hardware
- 32 Disabling Hardware
- 33 Removing Mac OS 9
- 33 Using the Command Line to Remove Mac OS 9
- 34 Running Mac OS 9 from a CD or DVD
- 34 Running Mac OS 9 from a Disc Image
- 35 Securing System Startup
- 36 Using the Open Firmware Password Application
- 37 Configuring Open Firmware Settings
- 38 Using Command-Line Tools to Secure Startup
- 38 Requiring a Password for Single-User Mode
- 39 Configuring Access Warnings
- 39 Enabling Access Warnings for the Login Window
- 40 Enabling Access Warnings for the Command Line

Chapter 4

- 41 **Securing Accounts**
- 41 Types of User Accounts
- 42 Guidelines for Creating Accounts
- 42 Defining User IDs
- 43 Securing Nonadministrator Accounts
- 45 Securing Administrator Accounts
- 46 Securing the System Administrator Account
- 47 Understanding Directory Domains
- 48 Understanding Network Services, Authentication, and Contacts
- 49 Configuring LDAPv3 Access
- 50 Configuring Active Directory Access
- 50 Using Strong Authentication
- 51 Using Password Assistant

52	Using Smart Cards
52	Using Tokens
52	Using Biometrics
53	Setting Global Password Policies
53	Storing Credentials
54	Using the Default User Keychain
55	Securing Keychain Items
56	Creating Additional Keychains
57	Using Portable and Network-Based Keychains

Chapter 5

59	Securing System Preferences
59	System Preferences Overview
61	Securing .Mac Preferences
63	Securing Accounts Preferences
66	Securing Appearance Preferences
67	Securing Bluetooth Preferences
68	Securing CDs & DVDs Preferences
69	Securing Classic Preferences
71	Securing Dashboard and Exposé Preferences
72	Securing Date & Time Preferences
74	Securing Desktop & Screen Saver Preferences
76	Securing Displays Preferences
76	Securing Dock Preferences
77	Securing Energy Saver Preferences
78	Securing International Preferences
79	Securing Keyboard & Mouse Preferences
80	Securing Network Preferences
82	Securing Print & Fax Preferences
84	Securing QuickTime Preferences
85	Securing Security Preferences
87	Securing Sharing Preferences
90	Securing Software Update Preferences
91	Securing Sound Preferences
92	Securing Speech Preferences
93	Securing Spotlight Preferences
95	Securing Startup Disk Preferences
96	Securing Universal Access Preferences

Chapter 6

97	Securing Data and Using Encryption
97	Understanding Permissions
97	Setting POSIX Permissions
98	Viewing POSIX Permissions
99	Interpreting POSIX Permissions

100	Modifying POSIX Permissions
100	Setting File and Folder Flags
100	Viewing Flags
100	Modifying Flags
101	Setting ACL Permissions
101	Enabling ACL
102	Modifying ACL Permissions
102	Setting Global File Permissions
103	Securing Your Home Folder
104	Encrypting Home Folders
105	Using FileVault Master Keychain
105	Encrypting Portable Files
106	Creating a New Encrypted Disk Image
107	Creating an Encrypted Disk Image from Existing Data
107	Creating Encrypted PDFs
108	Securely Erasing Data
109	Using Disk Utility to Securely Erase a Disk or Partition
109	Using Command-Line Tools to Securely Erase Files
110	Using Secure Empty Trash
111	Using Disk Utility to Securely Erase Free Space
111	Using Command-Line Tools to Securely Erase Free Space

Chapter 7

113	Securing Network Services
113	Securing Apple Applications
113	Securing Mail
114	Securing Web Browsing
115	Securing Instant Messaging
115	Securing VPN
117	Securing Firewall
118	About Internet Sharing
119	Enabling TCP Wrappers
120	Securing SSH
120	Enabling an SSH Connection
121	Configuring a Key-Based SSH Connection
124	Preventing Connections to Unauthorized Host Servers
125	Using SSH as a Tunnel
126	Securing Bonjour
127	Securing Network Services
127	Securing AFP
128	Securing Windows Sharing
128	Securing Personal Web Sharing
128	Securing Remote Login
129	Securing FTP Access

- 129 Securing Apple Remote Desktop
- 129 Securing Remote Apple Events
- 129 Securing Printer Sharing
- 129 Securing Xgrid
- 130 Intrusion Detection Systems

Chapter 8

- 131 **Validating System Integrity**
- 131 About Activity Analysis Tools
- 131 Using Auditing Tools
- 132 Configuring Log Files
- 132 Configuring syslogd
- 133 Local System Logging
- 134 Remote System Logging
- 135 About File Integrity Checking Tools
- 135 About Antivirus Tools

Appendix A

- 137 **Security Checklist**
- 137 Installation Action Items
- 138 Hardware and Core Mac OS X Action Items
- 138 Account Configuration Action Items
- 139 Securing System Software Action Items
- 139 .Mac Preferences Action Items
- 140 Accounts Preferences Action Items
- 140 Appearance Preferences Action Items
- 140 Bluetooth Preferences Action Items
- 141 CDs & DVDs Preferences Actions Items
- 141 Classic Preferences Action Items
- 142 Dashboard and Exposé Preferences Action Items
- 142 Date & Time Preferences Action Items
- 142 Desktop & Screen Saver Preferences Action Items
- 142 Dock Preferences Action Items
- 143 Energy Saver Preferences Action Items
- 143 Securing International Preferences
- 143 Securing Keyboard & Mouse Preferences
- 143 Network Preferences Action Items
- 144 Print & Fax Preferences Action Items
- 144 QuickTime Preferences Action Items
- 144 Security Preferences Action Items
- 145 Sharing Preferences Action Items
- 145 Software Update Preferences Action Items
- 145 Sound Preferences Action Items
- 145 Speech Preferences Action Items
- 146 Spotlight Preferences Action Items

	146	Startup Disk Preferences Action Items
	146	Data Maintenance and Encryption Action Items
	146	Network Services Configuration Action Items
	148	System Integrity Validation Action Items
Appendix B	149	Daily Best Practices
	149	Password Guidelines
	149	Creating Complex Passwords
	150	Using an Algorithm to Create a Complex Password
	151	Safely Storing Your Password
	151	Password Maintenance
	152	Email, Chat, and Other Online Communication Guidelines
	152	Computer Usage Guidelines
Glossary	155	
Index	167	

About This Guide

This guide provides an overview of features in Mac OS X that can be used to enhance security, known as hardening your computer.

This guide is designed to give instructions and recommendations for securing Mac OS X version 10.4 or later, and for maintaining a secure computer.

Target Audience

This guide is for users of Mac OS X version 10.4 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 at least some experience using the Terminal application's command-line interface. You should also be familiar with basic networking concepts.

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

What's New in Mac OS X Version 10.4

Mac OS X version 10.4 offers the following major security enhancements:

- **Access control lists.** Provide flexible file system permissions that are fully compatible with Windows Server 2003 Active Directory environments and Windows XP clients.
- **Secure instant messaging.** Your private, secure iChat Server, based on Jabber XMPP protocol, integrates with Open Directory for user accounts and authentication.
- **Software update server.** By enabling the new Apple Software Update Server, administrators can control which updates their users can access and when.
- **Certificate management.** Certificate Assistant is an easy-to-use utility that helps you request, issue, and manage certificates.
- **Smart cards as keychains.** Use a smart card to authenticate to your system or Keychain.

- **Secure erase.** Secure erase follows the U.S. Department of Defense standard for the sanitation of magnetic media.
- **VPN service is now Kerberized.** Use Kerberos-based authentication for single sign-on to a VPN network.
- **Firewall enhanced.** The firewall service has been enhanced to use the reliable open source IPFW2 software.
- **Antivirus and antispam.** New adaptive junk mail filtering using SpamAssassin and virus detection and quarantine using ClamAV.

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 with securing computers running Mac OS X Server version 10.4. or later, see *Mac OS X Server Security Configuration*.

This guide includes the following chapters, arranged in the order that you're likely to need them when securely configuring your computer:

- Chapter 1, "Introducing Mac OS X Security Architecture," explains the infrastructure of Mac OS X. It also discusses the different layers of security within Mac OS X.
- Chapter 2, "Installing Mac OS X," describes how to securely install Mac OS X. The chapter also discusses how to securely install software updates and explains permissions and how to repair them.
- Chapter 3, "Protecting Hardware and Securing Global System Settings," explains how to physically protect your hardware from attacks. This chapter also tells you how to secure settings that affect all users of the computer.
- Chapter 4, "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 5, "Securing System Preferences," describes recommended settings to secure all Mac OS X system preferences.
- Chapter 6, "Securing Data and Using Encryption," describes how to encrypt your data and how to use secure erase to ensure old data is completely removed.
- Chapter 7, "Securing Network Services," describes how to protect the computer by securely configuring network services.
- Chapter 8, "Validating System Integrity," 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, "Daily Best Practices," explains best practices for creating and managing passwords. It also discusses communication and computer usage guidelines.
- The Glossary defines terms you'll encounter as you read this guide.

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

Using This Guide

The following are 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 what security risks it might introduce and take measures to monitor or mitigate those risks.

Using Onscreen Help

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

Mac Help

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

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

The Mac OS X Server Suite

The Mac OS X Server documentation includes a suite of guides that explain the available services and provide instructions for configuring, managing, and troubleshooting the services. All of the guides are available in PDF format from: www.apple.com/server/documentation/

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

This guide ...	tells you how to:
<i>User Management</i>	Create and manage user accounts, groups, and computer lists. Set up managed preferences for Mac OS X clients.
<i>Web Technologies Administration</i>	Set up and manage a web server, including WebDAV, WebMail, and web modules.
<i>Windows Services Administration</i>	Set up and manage services including PDC, BDC, file, and print for Windows computer users.
<i>Xgrid Administration</i>	Manage computational Xserve clusters using the Xgrid application.
<i>Mac OS X Server Glossary</i>	Learn about terms used for server and storage products.

Getting Documentation Updates

Periodically, Apple posts new onscreen help topics, revised guides, and help topics. The new help topics include updates to the guides.

- To view new onscreen help topics, make sure your computer is connected to the Internet and access the Mac Help page.
- To download the latest guides and solution papers in PDF format, go to the Mac OS X Server documentation webpage: www.apple.com/server/documentation/.

Getting Additional Information

For more information, Apple provides the following resources:

- *Read Me documents*—Important updates and special information. Look for them on the installation discs.
- *Mac OS X Server website* (www.apple.com/server/macosx/)—Gateway to extensive product and technology information.
- *Apple Support website* (www.apple.com/support/)—Access to hundreds of articles from Apple’s support organization.
- *Apple Customer Training website* (train.apple.com)—Instructor-led and self-paced courses for honing your server administration skills.
- *Apple Certification Programs website* (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 Discussions website* (discussions.info.apple.com)—Discussions forums for sharing questions, knowledge, and advice with other administrators.
- *Apple Product Security Mailing Lists website* (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/)—Access to Darwin open source code, developer information, and FAQs.

- *Apple Product Security website* (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/)—The 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)—The National Institute of Standards and Technology repository for security configuration checklists.
- *DISA Security Technical Implementation Guide* (www.disa.mil/gs/dsn/policies.html)—The 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)—The Center for Internet Security benchmark and scoring tool used to establish CIS benchmarks.

Acknowledgments

Apple would like to thank the National Security Agency for their assistance in creating and editing the security configuration guides for Mac OS X 10.4 'Tiger' client and server.

Introducing Mac OS X Security Architecture

1

Mac OS X delivers the highest level of security through the adoption of industry standards, open software development, and smart architectural decisions.

With Mac OS X, a security strategy is implemented that is central to the design of the operating system, ensuring that your Mac is safe and secure. This chapter describes the features in Mac OS X that can be used to enhance security on your computer.

- **Open source foundation.** Using open source methodology makes Mac OS X a more 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.
- **Secure default settings.** When you take your Mac out of the box, it is securely configured to meet the needs of most common usage environments, so you don't have to be a security expert to setup your computer. The default settings make it very difficult for malicious software to infect your computer. Security can be further configured on the computer to meet organizational or user requirements.
- **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.
- **Innovative security applications.** Mac OS X includes features that take the worry out of using a computer. For example, FileVault protects your documents using strong encryption, an integrated VPN client gives you secure access to networks over the Internet, and a powerful firewall secures your home network.
- **Rapid response.** Because the security of your computer is so 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 any potential threats. Should vulnerabilities be discovered, the built-in Software Update tool automatically 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) and Common Data Security Architecture (CDSA). BSD is a form of the UNIX operating system that provides fundamental services, including the Mac OS X file system, and file access permissions. CDSA provides a much wider array of security services, including finer-grained access permissions, authentication of users' identities, encryption, and secure data storage. The default security settings on your Mac OS X computer are configured to be secure from local network and Internet attacks.

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 given Mach port (a Mach port represents a task or some other resource). BSD security policies and Mach access permissions constitute an essential part of security in Mac OS X, and are both critical to enforcing local security.

Access Permissions

An important aspect of computer security is the granting or denying of access permissions (sometimes called access rights). A permission is the ability to perform a specific operation, such as gaining access to data or to execute code. Permissions are granted at the level of folders, subfolders, files, or applications. Permissions are also granted for specific data within 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 the networking protocols.

Security Framework

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 many 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 freely 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 ensure that Mac OS X is truly secure.

This open approach has clear advantages and a long, well-documented history of quickly identifying and correcting source code that could potentially contain exploitable vulnerabilities. Mac OS X users can comfortably rely on the ongoing public examination by large numbers of security experts, which is made possible by Apple's open approach to software development. The result is an operating system that is inherently more secure.

Layered Security Defense

Mac OS X security is built on a layered defense for maximum protection. Security features 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—Authentication using keychains and encryption using FileVault helps prevent intruders from using your applications and viewing data on your computer.
- Secure network protocols—Secure sockets layer helps prevent intruders from viewing information exchange across a network and Kerberos secures the authentication process.
- Operating system—POSIX and ACL permissions help prevent intruders from accessing your files.
- Hardware—The Open Firmware Password application helps prevent people who can access your hardware from gaining root-level access permissions to your computer files.



Built-In Security Services

Mac OS X has several security services that are managed by the security server daemon. Security server implements several security protocols such as encryption, decryption, and authorization computation. The use of the security server to perform actions with cryptographic keys enables the security implementation to maintain the keys in a separate address space from the client application, keeping them more secure.

Keychain Services

A keychain is used to store passwords, keys, certificates, and other secrets. 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.

The Mac OS X keychain services enable you to create keychains and provide secure storage of keychain items. Once a keychain is created, you can add, delete, and edit keychain items, such as passwords, keys, certificates, and notes for one or more 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.

Secure Transport Services

Secure Transport is used to implement Secure Socket Layer (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.

Certificate, Key, and Trust Services

The certificate, key, and trust services include functions to:

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

These functions are carried out when the services call a variety of Common Security Service Manager (CSSM) functions. This is all transparent to users.

Authorization Services

Authorization services give applications control over access to specific operations within an application. For example, a directory application that can be started by any user can use authorization services to restrict access for modifying directory items to administrators. In contrast, BSD provides access permissions only to an entire file or application.

Smart Card Services

A smart card can be a plastic card (similar in size to a credit card) or a USB dongle that has memory and a microprocessor embedded in it. The smart card is capable of both storing information and processing it. Smart cards can securely store passwords, certificates, and keys. A smart card normally requires a personal identification number (PIN) or biometric measurement (such as a fingerprint) as an additional security measure. Because it contains a microprocessor, a smart card can carry out its own authentication evaluation offline before releasing information. Smart cards can exchange information with a computer through a smart card reader.

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 first authenticating the entity and then determining whether it has the appropriate permissions.

Authentication is the process of verifying the identity of a user or service. Authentication is normally done as a step in the authorization process. Some applications and operating system components carry out their own authentication. Authentication might use authorization services when necessary.

Though the default installation of Mac OS X is highly secure, it can be customized for your particular network security needs.

By securely configuring the different stages of the installation process and understanding Mac OS X permissions, you can make sure that your computer is hardened to match your security policy.

System Installation Overview

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

Because there might still be some recoverable data left on the computer, you should securely erase the partition that you're installing Mac OS X on. For more information, see "Using Disk Utility to Securely Erase a Disk or Partition" on page 109.

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 111.

Disabling the Open Firmware Password

Before installing Mac OS X, you should first disable the Open Firmware password.

If you already have Mac OS X version 10.4 installed, you can use the Open Firmware Password application to disable the Open Firmware password. For more information, see "Using the Open Firmware Password Application" on page 36.

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

To disable the Open Firmware password:

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

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

- 3 Enter the following commands:

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

Installing from CD or DVD

When you install Mac OS X version 10.4 from the original installation discs, you should do two things: erase the partition where you will install Mac OS X, and install only the packages that you plan on using.

Before installing Mac OS X, you should first 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 109.

WARNING: To install Mac OS X, you must erase the contents of the partition you’re installing on. Be sure to back up the files that you want to keep before continuing.

To install Mac OS X version 10.4 from the original installation discs:

- 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 will start up using the disc in the optical drive.
- 3 Follow the installation steps until you reach the “Select a Destination” step.
- 4 Choose a partition to install Mac OS X on, and click Options. Select “Erase and Install.” In “Format disk as,” choose “Mac OS Extended (Journaled).”
Mac OS Extended disk formatting provides extended file characteristics that enhance multiplatform interoperability.
- 5 Click OK and then click Continue.
- 6 In the “Easy Install on *partition_name*” step, click Customize. Deselect any packages that you do not plan on using. Do not select the X11 package unless you have a use for it.
The X11 X Window system lets you run X11-based applications in Mac OS X. While this might be useful, it also makes it harder to maintain a secure configuration.
Removing additional unused packages not only frees up disk space, but reduces the risk of attackers leveraging potential vulnerabilities in unused components.
- 7 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 that the network is isolated and can be trusted. For information about deploying images from a network, see the getting started guide. Verify the image to make sure that it is correct. For more information about verifying images, see “Verifying the Integrity of Software” on page 28.

Restoring from Preconfigured Disk Images

One of the most efficient ways to deploy secure computers is to configure a model computer first, using all of the security settings requested by your organization. Create a disk image of the computer after thoroughly testing the computer’s settings, making sure that the computer meets your organization’s standards. You can then deploy this image without having to manually configure individual settings on each computer.

You can use NetBoot or Apple Software Restore (ASR) to restore your computer from a network-based disk image. With NetBoot, you can restore an image directly from the network. With ASR, you can restore 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 deploying multiple computers simultaneously, ASR can be much more efficient.

For information about how to use NetBoot, see the system imaging and software update administration guide. For information about how to use ASR, enter `man asr` in a Terminal window. For information about how to use Disk Utility to create disk images, see the system imaging and software update administration guide.

Initializing System Setup

After installing Mac OS X, the computer restarts and loads Setup Assistant.

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 the Setup Assistant, but you should avoid entering any information considered sensitive by your organization.

To use Setup Assistant without providing confidential information:

- 1 Proceed to the Do You Already Own a Mac step. Select “Do not transfer my information,” and click Continue.

- 2 Proceed to the Your Internet Connection step. Click Different Network Setup. Select “My computer does not connect to the Internet,” and click Continue.

Even if you can configure the computer to access your network, you should disable network access until your network services settings are secure and validated. For more information, see Chapter 7, “Securing Network Services,” on page 113.

If you don’t disable your network connection, an additional step, Enter Your Apple ID, appears. Don’t enter any 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. 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 any settings. Before bypassing, you might want to go back through the steps to remove any sensitive information. Once you enter information in the Your Internet Connection step, you cannot go back to that step to change your network settings. You can then only change network settings after completing installation.

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

Creating Initial System Accounts

After completing the initial steps of Setup Assistant, you’re presented with the Create Your Account step. In this step, you create a system administrator account. You should make sure that this account is as secure as possible.

Note: The system administrator account should be used only for performing administrative tasks. You should also create additional accounts for nonadministrative use. For more information, see “Types of User Accounts” on page 41.

To set up a secure system administrator account:

- 1 In the Name and Short Name fields, enter names that are not easily guessed. Avoid easily guessed names and short names like “administrator” and “admin.” You can use either the long name or the short name when you’re authenticating. The short name is often used by UNIX commands and services.
- 2 In the Password and Verify fields, enter a complex password that is at least twelve characters long and composed of mixed-cased characters, numbers, and special characters (such as ! or @).

Mac OS X supports only passwords that contain standard ASCII characters.

For more information, see “Creating Complex Passwords” on page 149.

- 3 In the Password Hint field, do not enter any information related to your password. If a hint is provided, the user is presented with the hint after three failed authentication attempts. Any password-related information provided in the field could compromise the integrity of the password. Adding contact information for your organization's technical support line would be convenient and doesn't compromise password integrity.
- 4 Click Continue.

Setting Correct Time Settings

After creating the system administrator account, you'll 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 automatically 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 72.

Updating System Software

After installing Mac OS X, be sure to install the latest approved security updates. Mac OS X includes Software Update, an application that downloads and installs software updates either from Apple's Software Update server or from an internal software update server. You can configure Software Update so that it checks for updates either periodically or whenever you choose. You can also configure Software Update to download, but not install, updates, in case 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 prequalify software updates against organization configurations before updating individual systems.

System updates should be installed immediately after the operating system installation. 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

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

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

Important: If you have not secured and validated your settings for network services you should not enable your network connection to install software updates. For information, see Chapter 7, “Securing Network Services,” on page 113. Until you have securely configured your network services settings, you will be limited to using the manual method of installing software updates.

For more information, see “Securing Software Update Preferences” on page 90.

Updating from an Internal Software Update Server

Your computer automatically looks 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 run a chance of downloading malicious updates from a rogue software update server. Software Update, however, will not install a package that has not been digitally signed by Apple.

If you connect your computer to a network that manages its client computers, the network can require that the computer use a specified software update server. Or, you can enter the following command in a Terminal window to specify your software update server:

```
defaults write com.apple.SoftwareUpdate CatalogURL http://  
    swupdate.apple.com:8088/index.sucatalog
```

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

Updating from Internet-Based Software Update Servers

Before connecting to the Internet, make sure your network services are securely configured. For information, see Chapter 7, “Securing Network Services,” on page 113.

Instead of using your operational computer to check for and install updates, consider using a test-bed computer to download updates and verify file integrity before installing updates. 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 27.

You can also download software updates for all of Apple’s products at www.apple.com/support/downloads/.

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 all updates. To get older versions of updates, go to the software update website at 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 /Library/Packages/ folder. If you do not want to install any of the updates, click Quit.
- 3 Accept the licensing agreements to start installation.

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

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

Updating Manually from Installer Packages

Software updates can be manually downloaded for all of Apple’s products from www.apple.com/support/downloads/ using a computer designated specifically for downloading and verifying updates. The download should be done separately so that file integrity can be verified before the updates are installed.

It is possible to 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/ and click the “Security Updates page” link.

To manually download, verify and install software updates:

- 1 Go to www.apple.com/support/downloads/ and download the necessary software updates on a computer designated for verifying software updates.

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

- 2 Review the SHA-1 digest (also known as a checksum) for each update file downloaded, which should be posted online with the update package.
- 3 Check all downloaded updates for viruses.
- 4 Verify the integrity of each update.
For more information, see “Verifying the Integrity of Software” on page 28.
- 5 Transfer the update packages from your test computer to your current computer. The default download location for update packages is `/Library/Packages/`. You can transfer update packages to any location on your computer.
- 6 Double-click the package. If the package is located within a disk image (dmg) file, double-click the dmg file, and then double-click the package.
- 7 Proceed through the installation steps.
- 8 Restart the computer, if requested.

Install the appropriate system update and then install any subsequent security updates. These updates should be installed in order by release date, oldest to newest.

Verifying the Integrity of Software

Software images and updates can include a SHA-1 digest, which is also known as a 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.

To verify software integrity:

- 1 Open Terminal.
- 2 Use the `sha1` command to display a file's SHA-1 digest.

```
$ /usr/bin/openssl sha1 full_path_filename
```

The *full_path_filename* is the full path filename of the update package or image for which the SHA-1 digest is being checked.

If provided, the SHA-1 digest for each software update or image should match the digest created for that file. If it does not, the file was corrupted in some way and a new copy should be obtained.

Repairing Disk Permissions

Before you modify or repair disk permissions, you should understand Portable Operating System Interface (POSIX) and Access Control List (ACL) permissions. POSIX permissions are standard for UNIX operating systems. ACL permissions are used by Mac OS X, and are compatible with Windows Server 2003 and Windows XP.

Kinds of Permissions

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

- 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.

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).

POSIX Permissions Overview

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

For more information, see “Setting POSIX Permissions” on page 97.

ACL Permissions Overview

Access Control List 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 and Windows XP, giving you added flexibility in a multiplatform environment.

ACLs provide more granularity when assigning privileges than POSIX permissions. For example, rather than giving a user full write permission, you can restrict him or her to the creation of only folders and not files.

If a file or folder has no ACEs defined for it, Mac OS X applies the standard POSIX permissions. If a file or folder has one or more ACE 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 the ACEs, Mac OS X evaluates the 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 101.

Using Disk Utility to Repair Disk Permissions

Installing software sometimes causes file permissions to become incorrectly set. Incorrect file permissions can create security vulnerabilities. Disk Utility repairs only POSIX permissions or the 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 stored in the packages receipt file. Each Bill of Materials file contains a list of the files installed by that package, along with the proper permissions for each file.

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

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

Note: If you’ve modified permissions for files, in accordance with organizational policies, be aware that repairing disk permissions can reset those modified permissions to those stated in the “Bill of Materials” files. After repairing permissions, you should re-apply the file permission modifications to stay within your organizational policies.

To repair disk permissions:

- 1 Open Disk Utility.
- 2 Select the partition that you want to repair.
Be careful to select a partition, not a drive. Partitions are contained within drives and are indented one level in the list on the left.
- 3 Click Repair Disk Permissions.
If you do not select a partition, this button is disabled.
- 4 Choose Disk Utility > Quit Disk Utility.
- 5 Choose Installer > Quit Installer, and click Restart.

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

This chapter discusses common practices for protecting hardware and demonstrates how to remove Mac OS 9 and secure both Open Firmware and Mac OS X startup. This chapter also discusses how using log files help to monitor system activity.

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 various 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, or bolt or fasten it to a wall or piece of furniture.

The hard drive is the most critical hardware component in your computer. Take special care to prevent access to the hard drive. If someone removes your hard drive and installs it in another computer, they can bypass any safeguards you set up. Lock or secure the computer's internal hardware. If you can't guarantee the physical security of the hard drive, consider using FileVault for each home folder (FileVault encrypts home folder content and prevents the content from being compromised). For more information, see "Encrypting Home Folders" on page 104.

If you have a portable computer, keep it secure. Lock up the computer or hide the computer 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.

Disabling Hardware

Hardware components such as wireless features and microphones should be physically disabled if possible. Only an Apple Certified Technician should physically disable these components, which may not be practical in all circumstances. The following instructions provide an alternative means of disabling these components by removing the associated kernel extensions. Removing the kernel extensions does not permanently disable the components; however, administrative access is needed to restore and reload them. Although disabling hardware in this manner is not as secure as physically disabling hardware, it is more secure than only disabling hardware through the System Preferences. This method of disabling hardware components may not be sufficient to meet site security policy. Consult operational policy to determine if this method is adequate.

The following instructions will remove AirPort, Bluetooth, the microphone, and support for an external iSight camera. This will not remove the support for the internal iSight cameras currently shipping on some Macintosh systems. There is currently no way to disable this camera in software without disabling all USB drivers, which will also disable the keyboard, mouse, etc.

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

To remove kernel extensions for certain hardware:

- 1 Open the `/System/Library/Extensions` folder.
- 2 To remove AirPort support, drag the following files to the Trash:
 - AppleAirPort.kext
 - AppleAirPort2.kext
 - AppleAirPortFW.kext
- 3 To remove support for Bluetooth, drag the following files to the Trash:
 - IOBluetoothFamily.kext
 - IOBluetoothHIDDriver.kext
- 4 To remove support for audio components such as the microphone, drag the following files to the Trash:
 - AppleOnboardAudio.kext
 - AppleUSBAudio.kext
 - AudioDeviceTreeUpdater.kext
 - IOAudioFamily.kext
 - VirtualAudioDriver.kext
- 5 To remove support for the iSight camera, drag the following file to the Trash:
 - Apple_iSight.kext

- 6 (Optional) To remove support for mass storage devices (e.g. USB flash drives, external USB hard drives, external FireWire Hard Drives), drag the following files to the Trash:
IOUSBMassStorageClass.kext
IOFireWireSerialBusProtocolTransport.kext
- 7 Open the `/System/Library` folder.
- 8 Drag the following files to the Trash:
Extensions.kextcache
Extensions.mkext
- 9 Choose `Finder > Secure Empty Trash` to delete the file.
- 10 Restart the system.

Removing Mac OS 9

When you upgrade from previous versions of Mac OS X to Mac OS X version 10.4, an adaptation of Mac OS 9, known as Classic, remains on the computer. If you perform a new installation of Mac OS X version 10.4 without upgrading, Mac OS 9 is not installed on the computer. It is possible to install Mac OS 9 on computers with a new installation of Mac OS X version 10.4.

Mac OS 9 lacks many of the security features included with Mac OS X, so you should remove it unless you need it. If you must use Mac OS 9, you can run it from a CD or DVD, or from a disc image.

Using the Command Line to Remove Mac OS 9

To remove Mac OS 9, use the command line. You must log in as an administrator who can use the `sudo` command to remove files. For more information, see “Securing the System Administrator Account” on page 46.

WARNING: Incorrectly entering any of the commands described in this task can erase critical data. Pay particular attention to correctly entering single quotes. Misplacing these single quotes can result in the removal of Mac OS X or applications.

To remove Mac OS 9 and Mac OS 9 applications and files:

- 1 Log in to Mac OS X as an administrator who can use `sudo` to remove files.
By default, all users who are administrators can use the `sudo` command to remove files. If you modify `/etc/sudoers`, you can choose which users can use `sudo`. For information about how to modify the `/etc/sudoers` file, enter `man sudoers` in a Terminal window.
- 2 Open Terminal.
- 3 Enter the following command to remove the Classic icon from System Preferences:

```
$ sudo srm -rf '/System/Library/PreferencePanes/Classic.prefPane'
```

- 4 Enter the following commands to remove Classic folders and files:

```
$ sudo srm -rf '/System/Library/Classic/'
$ sudo srm -rf '/System/Library/CoreServices/Classic Startup.app'
% sudo srm -rf '/System/Library/UserTemplate/English.lproj/Desktop/Desktop
(Mac OS 9)'
```

- 5 Enter the following commands to remove Mac OS 9 folders and files:

```
$ sudo srm -rf '/System Folder'
$ sudo srm -rf '/Mac OS 9 Files/'
```

- 6 Enter the following command to remove Mac OS 9 applications:

```
sudo srm -rf '/Applications (Mac OS 9)'
```

- 7 Restart the computer.

Running Mac OS 9 from a CD or DVD

Classic is an environment for running Mac OS 9 applications. If you must run Mac OS 9, you can use Classic to run it from a CD or DVD. By running Mac OS 9 from a CD or DVD, you enforce read-only access.

Note: Intel-based Macintosh computers do not support the Classic environment or Mac OS 9.

To run Mac OS 9 from a CD or DVD:

- 1 Install Mac OS 9 and the software that requires Mac OS 9 on a test-bed computer.
- 2 Burn the Mac OS 9 System Folder from the test-bed computer onto a blank CD or DVD. The System Folder is located at the root level of a partition. It might be named something besides “System Folder.” System folders are denoted by a folder icon with a 9 superimposed on them.
- 3 Eject the CD or DVD from the test-bed computer and insert it into your operational computer.
- 4 Open Classic preferences on your operational computer.
- 5 Select the System Folder located on the CD or DVD in the “Select a system folder for Classic” list.
- 6 Click Start.

Running Mac OS 9 from a Disc Image

Classic is an environment for running Mac OS 9 applications. If you must run Mac OS 9, you can use Classic to run it from a disc image. By running Mac OS 9 from a disc image, you enforce read-only access.

Note: Intel-based Macintosh computers do not support the Classic environment or Mac OS 9.

To run Mac OS 9 from a disc image:

- 1 Install Mac OS 9 and the software that requires Mac OS 9 on a test-bed computer.
- 2 On the test-bed computer, create a folder and name it Mac OS 9.
- 3 Copy the Mac OS 9 System Folder into the Mac OS 9 folder you created in the previous step.
- 4 On the test-bed computer, open Disk Utility.
- 5 Choose File > New > Disk Image from Folder.
- 6 Select the Mac OS 9 folder (created in step 2) and click Image.
- 7 In Image Format, choose read-only.
- 8 In Encryption, choose none.
- 9 Click Save.
- 10 Copy the Mac OS 9 disc image to your operational computer.
- 11 Double-click the Mac OS 9 disc image to mount it.
- 12 Open Classic preferences on your operational computer.
- 13 Select the System Folder located on the mounted disc image in the “Select a system folder for Classic” list.
- 14 Click Start.

Securing System Startup

When a computer starts up, it first starts either Open Firmware or Extensible Firmware Interface (EFI). EFI is similar to Open Firmware, but it runs on Intel-based Macintosh computers. Open Firmware or EFI determines which partition or disk to load Mac OS X from. They also allow (or prevent) the user to enter single-user mode.

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

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

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

To secure startup, perform one of the following tasks:

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

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

Open Firmware password protection can be bypassed if the user changes the physical memory configuration of the machine and then resets the PRAM three times (by holding down Command, Option, P, and R keys during system startup). An Open Firmware password will provide some protection, however, it can be reset if a user has physical access to the machine and can change the physical memory configuration of the machine.

You can require a password to start single-user mode, which would further secure your computer.

For more information about Open Firmware password protection, see AppleCare Knowledge Base article #106482, “Setting up Open Firmware Password protection in Mac OS X 10.1 or later” (www.apple.com/support/), and AppleCare Knowledge Base article #107666, “Open Firmware: Password Not Recognized when it Contains the Letter ‘U’” (www.apple.com/support/).

Using the Open Firmware Password Application

The Mac OS X installation disc includes Open Firmware Password application, an application that allows you to enable an Open Firmware or EFI password.

To use the Open Firmware Password application:

- 1 Log in with an administrator account and open Open Firmware Password application (located on the Mac OS X installation disc in /Applications/Utilities/).
- 2 Click Change.
- 3 Select “Require password to change Open Firmware settings.”
To disable the Open Firmware or EFI password, deselect “Require password to change Open Firmware settings.” You won’t have to enter a password and verify it. Disabling the Open Firmware password is only recommended for when you install Mac OS X.
- 4 Enter a new Open Firmware or EFI password in the Password and Verify fields. Click OK.
This password can be up to eight characters.

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

- 5 Close the Open Firmware Password application.

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 Open Firmware Password application completed successfully.

Configuring Open Firmware Settings

You can securely configure Open Firmware settings within Open Firmware.

Note: If you are using an Intel-based Macintosh computer, you cannot use the following method to change the Open Firmware password. Use the Open Firmware Password application instead.

To configure Open Firmware settings within Open Firmware:

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

This loads Open Firmware.

- 2 At the prompt, change the password:

```
> password
```

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

This password can be up to eight characters.

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

- 4 Enable command mode:

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

In command mode, the computer will only start up from the partition selected in the Startup Disk pane of System Preferences.

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

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

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

```
> reset-all
```

The login window should appear after restarting.

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 appears, your Open Firmware settings are set correctly.

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

Using Command-Line Tools to Secure Startup

Open Firmware can also be configured throughout the command line by using the `nvr` tool. However, only the `security-mode` environment variable can be securely set. The `security-password` variable should not be set from the `nvr` tool, or it will be visible when viewing the environment variable list. To set the password for Open Firmware, start the computer in Open Firmware and set the password. See the “Configuring Open Firmware Settings” on page 37 for more information. The `nvr` tool requires system administrator or root access to set environment variables.

Note: If you are using an Intel-based Macintosh computer, you cannot use the following method to change secure startup. Use the Open Firmware Password application instead.

To use `nvr` to secure startup from the command line:

- 1 Set the security mode by entering the following command.

```
# nvr security-mode="command"
```

If you want to set the security mode to `full`:

```
# nvr security-mode="full"
```

- 2 Verify that the variable has been set. The following command displays a list of all the environment variables excluding the `security-password` variable.

```
# nvr -p
```

Requiring a Password for Single-User Mode

Additional protection can be provided in case the Open Firmware (PowerPC-based systems) or EFI (Intel-based systems) password is bypassed. By requiring entry of the root password during a single-user mode boot, the system can prevent automatic root login if the OF/EFI password is compromised.

To require entry of the root password during a single-user mode boot, the console and `ttys` must be marked as insecure in `/etc/ttys`. In fact, the system will require entry of a special root password, stored in `/etc/master.passwd`. If this remains unset as recommended, then it will be impossible for a user to enter the root password and complete the single-user boot, even if the Open Firmware password protection was bypassed.

To require entry of the root password for single-user mode:

- 1 Log in as an administrator.
- 2 Start the Terminal application, located in /Applications/Utilities.
- 3 At the prompt, enter the command:

```
$ cd /etc
```
- 4 To create a backup copy of /etc/ttys, enter the command:

```
$ sudo mv ttys ttys.old
```
- 5 To edit the ttys file as root, enter the command:

```
$ sudo pico ttys
```
- 6 Replace all occurrences of the word “secure” with the word “insecure” in the configuration lines of the file. Any line that does not begin with a “#” is a configuration line.
- 7 Exit, saving changes.

Configuring Access Warnings

You can use a login window warning 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, check your organization’s policy for what to use as your access warning.

When a user tries to access the computer’s login window (either locally or through Apple Remote Desktop), the user will see the access warning you create.



To create a login window access warning:

1 Open Terminal.

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.

Your logged-in account must be able to use `sudo` to perform a `defaults write`.

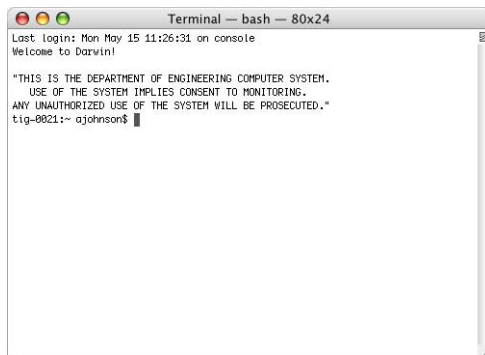
3 Log out to test your changes.

Your access warning text appears below the Mac OS X subtitle.

Enabling Access Warnings for the Command Line

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

When a user opens Terminal locally or connects to the computer remotely, the user sees the access warning you create.



To create a command-line access warning:

1 Open Terminal.

2 Open the file `/etc/motd` in a text editor:

```
$ sudo pico /etc/motd
```

You must be able to use `sudo` to open `pico`. For information about how to use `pico`, enter `man pico` in a Terminal window.

3 Replace any existing text with your access warning text.

4 Save your changes and exit the text editor.

5 Open a new Terminal window to test your changes.

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

Securely configuring user accounts requires determining how the accounts will be used and setting the level of access for users.

When you define a local user's account, you specify the information needed to prove the user's identity: user name, authentication method (such as a 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 can use either a nonadministrator account or an administrator account. The main difference between the two types of accounts is that Mac OS X provides safety mechanisms to prevent nonadministrator users from editing key preferences, or from performing certain actions that are critical to computer security. Administrator users are not as limited as nonadministrator users.

The nonadministrator and administrator accounts can be further defined by specifying additional user privileges or restrictions.

User Account	User Access
Standard nonadministrator	Nonprivileged user access
Managed nonadministrator	Restricted user access
Administrator	Administer the computer configuration
System administrator (root)	Unrestricted access to the entire computer

Unless administrator access is required, you should always log in as a nonadministrator user. You should log out of the administrator account when you are not using the computer as an administrator. If you are logged in as an administrator, you are granted some privileges and abilities that you might not need. For example, you can modify some system preferences without being required to authenticate. This automatic 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 to each user account, but if several users share the same account, it becomes much more difficult to track which user performed a certain activity. Similarly, if several administrators share a single administrator account, it becomes much 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 one of the users sharing the account.

- Each user needing administrator access should have an individual 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 inadvertently 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 keep track of 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 file permissions.

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 do not want the user to appear in the login window of computers with Mac OS X version 10.4 or later installed, assign a user ID of less than 500.

In general, once a user ID has been 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 created on different servers onto one new server or cluster of servers. The same user ID might have been associated with a different user on the previous server.

Securing Nonadministrator Accounts

There are two types of nonadministrator accounts: standard and managed. Standard users don't have administrator privileges, and don't have any parental controls limiting their actions. Managed users also don't have administrator privileges, but they have active parental controls. Parental controls help deter unsophisticated users from performing any malicious activities. They can also help prevent users from accidentally 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 is managed through the network.

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



To secure a managed account:

- 1 Open Accounts preferences.
- 2 Click the lock to authenticate. Enter an administrator's name and password and click OK.

You can also authenticate through the use of a digital token, smart card, or biometric reader.
- 3 Select an account labeled "Standard" or "Managed."

You cannot set parental controls on administrator users. When selecting a user with the "Managed" label, make sure you do not select an account with preferences managed through the network.
- 4 Click Parental Controls.
- 5 Select Finder & System, and click Configure.
- 6 Click Some Limits.

You can also enable Simple Finder, which restricts an account to using only applications listed in the Dock. With Simple Finder enabled, users cannot create or delete files. Simple Finder also prevents users from being able to change their own passwords. Enabling Simple Finder is not recommended, unless your computer is used in a kiosk-like environment.
- 7 Select "Open all System Preferences" and "Change password."

To enable "Change password," you must enable "Open all System Preferences." By allowing the user to open all System Preferences, you also allow the user to change settings for things like screen saver activation. These settings can impact security. However, the inability of a user to change his or her own password is also a security risk.
- 8 Deselect "Burn CDs and DVDs."
- 9 Deselect "Administer printers."
- 10 Deselect "Allow supporting programs."

If you allow supporting programs, applications can load "helper" applications. If these helper applications are insecure, they can expose your computer to other security risks. These helper applications are loaded by an application, not by you, so you might not be aware of them running.
- 11 Select "This user can only use these applications."
- 12 Deselect applications and utilities that are not approved for use.

When you install third-party applications, they may be added to this list. You should disable all third-party applications unless the user has a specific need to use the 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. Additionally, if you're connecting to an organization's network, you should install only third-party applications that are specifically approved by the organization.

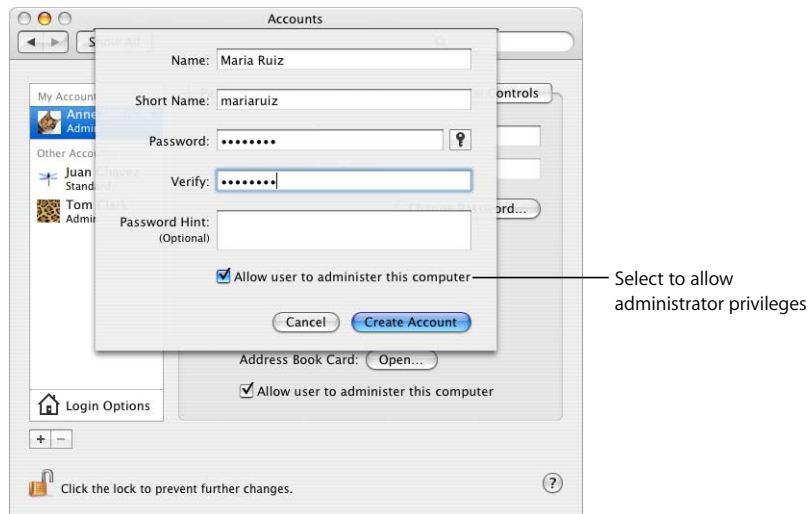
- 13 Deselect "Applications (Mac OS 9)" and "Others."
- 14 Click OK.

Securing Administrator Accounts

A user account with administrator privileges can perform all standard user-level tasks, and key administrator-level tasks, such as:

- Create user accounts
- Change the FileVault master password
- Enable or disable sharing
- Enable, disable, or change firewall settings
- Change other protected areas within System Preferences
- Install system software

In addition to restricting the distribution of administrator accounts, you should also limit the use of administrator accounts. Each administrator should have two accounts: a standard account for daily use, and an administrator account for when administrator access is needed.



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, any actions that involve critical system files require that you perform those actions as root. Even if you are logged in as a Mac OS X administrator, you still have to perform these commands as root, or by using the `sudo` command. Mac OS X logs all actions performed using the `sudo` command. This helps you track any misuse of the `sudo` command on a computer.

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

If multiple users can log in as root, it is impossible to track which user performed root actions. Direct root login should not be allowed, because the logs cannot identify which administrator logged in. Instead, accounts with administrator privileges should be used for login, and then the `sudo` command used to perform actions as root. For instructions about how to restrict root user access in NetInfo Manager, open Mac Help and search for “NetInfo Manager.”

By default, `sudo` is enabled for all administrator users. From the command line, you can disable root login or restrict the use of `sudo` command.

The computer uses a file named `/etc/sudoers` to determine which users have the authority to use `sudo`. You can modify root user access by changing the `/etc/sudoers` file to restrict `sudo` access to only certain accounts, and allow those accounts to perform only specifically allowed commands. This granularity gives you fine control over what users can do as root. For information about how to modify the `/etc/sudoers` file, see the `sudoers` man page.

The list of administrators allowed to use `sudo` should be limited to only those administrators who require the ability to run commands as root.

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

- 1 Edit the /etc/sudoers file using the `visudo` tool, which allows for safe editing of the file. The command must be run as root:

```
$ sudo visudo
```

- 2 Enter the administrator password when prompted.

Note: 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. See the `sudo` and `sudoers` man pages for more information.

- 3 In the Defaults specification section of the file, add the following line:

```
Defaults timestamp_timeout=0
```

This limits the use of the `sudo` command to a single command per authentication.

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

```
USER ALL=(ALL) ALL
```

Doing this means that any time a new administrator is added to the computer that administrator must be added to the /etc/sudoers file as described above, if that administrator requires the ability to use `sudo`.

- 5 Save and quit `visudo`.

For more information, enter `man vi` or `man visudo` in a Terminal window.

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 has to connect to the network and upload the file.

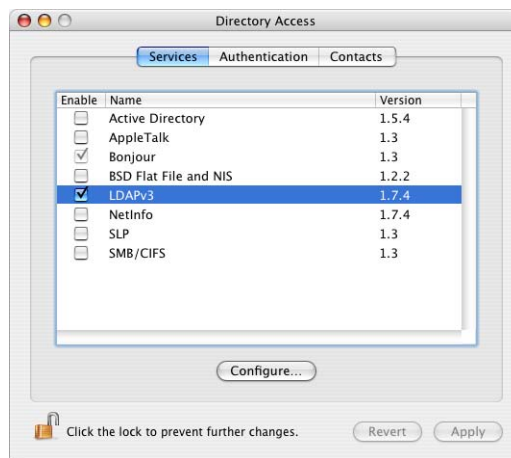
Network-based accounts are hosted in a network-based directory domain. When you log in to a network-based account, you authenticate with the network-based directory domain. Users with network accounts typically have network home folders. When they save files in their network home folders, the files are stored on the server.

Mobile accounts cache authentication information and managed preferences. A user's authentication information is maintained on the directory server, but 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 he or she is not connected to the network.

Users with mobile accounts have both local and network home folders, which combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders.

Understanding Network Services, Authentication, and Contacts

You can use Directory Access to configure your computer to use a network-based directory domain. Directory search services that are not used should be disabled in the Services pane of Directory Access.



Each kind of directory service and service discovery protocol can be enabled or disabled in Directory Access. Mac OS X doesn't access disabled directory services, except for the local NetInfo directory domain, which is always accessed. Mac OS X also doesn't try to discover network services using disabled service discovery protocols. However, disabling a service discovery protocol doesn't prevent Mac OS X from getting or providing network services. For example, if Bonjour is disabled, Mac OS X doesn't use it to discover file services, but you can still share your files and connect to file servers whose addresses you know.

In addition to enabling and disabling services, you can use Directory Access to choose the directory domains that you want to authenticate with. Directory Access 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 Access 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 either finds the information it needs or reaches the end of the list without finding the information.

For more information about using Directory Access, see the Open Directory administration guide.

Configuring LDAPv3 Access

Mac OS X version 10.4 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 your LDAPv3 security. Check with your network administrator to make sure your settings match your network's required settings.

When configuring LDAPv3, you should not add DHCP-supplied LDAP servers to automatic search policies. Otherwise, a malicious individual can create a rogue DHCP server and a rogue LDAP directory and then control your computer as the root user.

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

Configuring Active Directory Access

Connecting to an Active Directory server is not as secure as connecting to an Open Directory server that has all of its security settings enabled. For example, you cannot receive directory services from an Active Directory server that enables digitally signing or encrypting all packets.

Mac OS X 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. Mutual authentication automatically 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. Check with your network administrator to make sure your settings match your network's required settings. However, the "Allow administration by" setting can cause security issues because it allows any member of those groups to have administrator privileges on your computer. Additionally, you should only connect to trusted networks.

For more information about using Directory Access to connect to Active Directory servers, see the Open Directory administration guide.

Using Strong Authentication

Authentication is the process of verifying the identity of a local or network 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.

Passwords can be required 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 emerging authentication methods, such as smart cards, digital tokens, and biometric readers.

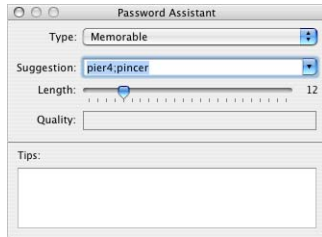
Strong authentication is created by using combinations of the following three authentication dimensions:

- What the user knows, such as a password or PIN number
- What the user has, such as SecurID card, smart card, or drivers license
- what the user is, such as a fingerprint, retina, or DNA

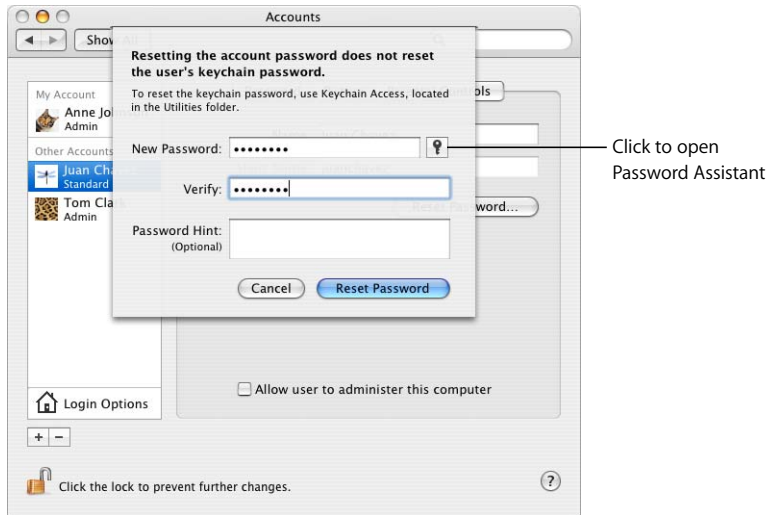
Using a combination of the three dimension above makes authentication more reliable and user identification more certain.

Using Password Assistant

Mac OS X includes Password Assistant, an application that analyzes the complexity of a password or generates a complex password for you. You can specify the length and type of password you'd like to generate. For example, you can create a randomly generated password, or a FIPS-181 compliant password.



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



For more information, see "Creating Complex Passwords" on page 149.

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 is capable of storing and processing 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 will process information, you must authenticate with the smart card by either a personal identification number (PIN) or biometric measurement (such as a fingerprint), which provides an additional layer of security.

For more information, see the *Smart Card Setup Guide* located on the web at www.apple.com/itpro/federal/.

Using Tokens

A digital token is used to identify a user for commerce, communication, or access control. This token can be generated by either software or hardware. Some of the most common tokens are the RSA SecurID and the CRYPTOCARD KT-1. These are hardware devices that automatically 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 will have different tokens.

You can use tokens for two-factor authentication. *Two-factor* refers to authenticating both through something you have (a One-Time-Password token) and something you know (a fixed password). The use of tokens increases the strength of the authentication process.

Tokens are frequently used for VPN authentication. For information, see “Securing VPN” on page 115.

Using Biometrics

Mac OS X supports emerging biometrics-based authentication technologies, such as thumbprint readers. Password-protected websites and applications can now be accessed without having to remember a long list of passwords. Some biometric devices allow you to authenticate simply 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 adds an additional factor to authentication by use of something you are (fingerprint).

Setting Global Password Policies

You can use the `pwpolicy` command-line tool to configure a password policy that can apply globally or to individual users. Global password policies are not implemented in Mac OS X; instead, password policies are set for each individual 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 twelve characters and have no more than three failed login attempts, enter the following in a Terminal window, where *authenticator* is the authenticator's name.

```
$ pwpolicy -a authenticator -setpolicy "minChars=12  
maxFailedLoginAttempts=3"
```

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

Storing Credentials

Mac OS X includes Keychain Access, an application that manages collections of passwords and certificates into 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 any other private values (called secure notes). These values are accessible only by unlocking the keychain using the keychain password and only by applications that have been 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 new key item in any user-created keychain. When an application must store an item in a keychain, it stores it in the one designated as your default. The default keychain is the keychain named "login," but you can change that to any user-created keychain. The default keychain is denoted by the name being displayed in bold.

Each item on the keychain has an 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 having to remember many passwords is that you're likely to either make all the passwords identical or keep a written list of all passwords. By using keychains, you can greatly reduce the number of passwords that you have to remember. Since you no longer have to remember passwords for a multitude of accounts, the passwords chosen can be very complex and could even be randomly generated.

Keychains provide some additional protection for passwords, passphrases, certificates, and other credentials stored on the computer. In some cases, such as using a certificate to sign an email message, the certificate must be stored in a keychain. If a credential must be stored on the computer, it should be stored and managed using Keychain Access. Check your organization's policy on keychain use.

Using the Default User Keychain

When a user's account is first created, a single, 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 automatically unlocked when the user logs in. It remains unlocked unless the user locks it, or until the user logs out.

The settings for the login keychain should be changed, so that the user will be required to unlock the login keychain 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 new password for the login keychain.

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

You can use Password Assistant to help you create a more secure password. For information, see "Using Password Assistant" on page 51.

- 6 Choose Edit > Change Settings for Keychain "login."
- 7 Select "Lock when sleeping."
- 8 Deselect "Synchronize this keychain using .Mac."

- 9 Secure each individual login keychain item.

For information, see “Securing Keychain Items” on page 55.

Securing Keychain Items

Keychains can store multiple encrypted items. You can configure some of these individual items so that only certain applications are permitted access. Access Control cannot be set for certificates.

To secure individual keychain items:

- 1 In Keychain Access, select a keychain, and then select an item.
- 2 Click the Information (i) button.
- 3 Click Access Control. Authenticate if you are requested to do so.
- 4 Select “Confirm before allowing access.”

After you enable this option, Mac OS X prompts you before giving a security credential to an application.

If you selected “Allow all applications to access this item” you allows any application to access the security credential whenever 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 selecting this, you have to provide the keychain password before applications can access security credentials. Enabling this is particularly important for critical items, such as your personal identity (your public key certificates and the corresponding private key), that are needed when signing or decrypting information. These items can also be placed in their own keychains.

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

Any application listed here will be prompted to enter the keychain password to access the security credentials.

Creating Additional Keychains

When a user account is created, it contains only the initial default keychain, login.

A user can create additional keychains, each of which can have different settings and purposes.

For example, a user might want to group all his or her credentials for mail accounts into one keychain. Since mail programs query the server frequently to check for new mail, it would not be practical to expect the user to reauthenticate every time such a check is being performed. The user could create a keychain and configure its settings, such that he or she would be 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 particular credential can automatically access it. This would force all 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 would be more appropriately stored 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 your keychains based on sensitivity, you prevent the exposure of your more 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 and select a new location for the keychain. Click Create.
- 3 Enter a password and verify it. 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*." 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 somewhat frequently, select "Lock after # minutes of inactivity" and select an appropriate 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 select an appropriate value, such as 1.

- 8 Select “Lock when sleeping.”
- 9 Drag the desired security credentials from other keychains to the new keychain. 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 individual item in the security credentials for your keychain.
For information, see “Securing Keychain Items” on page 55.

Using Portable and Network-Based Keychains

If you’re using a portable computer, consider storing all your keychains on a portable drive, such as a USB flash memory drive. The portable drive can be removed from the portable computer and stored separately when the keychains are not in use. Anyone attempting to access data on the portable computer will need the portable computer, the portable drive, and the 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, you’ll have to move all 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, it is possible to store keychains in other locations.

You can further protect portable keychains by storing them on biometric USB flash memory drives, or by storing your portable drive contents in an encrypted file. For information, see “Encrypting Portable Files” on page 105.

Check with your organization to see if they allow you to use 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 that you want to set up. The default location is /System/Library/Keychains/. Click Cancel.
- 5 Select the keychain that you want set up.

- 6 Choose File > Delete Keychain "*keychain_name*."
- 7 Click Delete References.
- 8 Copy the keychain files from the previously noted location to the portable drive.
- 9 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 110.

- 10 Open Finder, and double-click the keychain file located on your portable drive to add it to your keychain.

Securing Mac OS X system software enables further protection against attacks.

System Preferences has many different configurable preferences within it that can be used to further enhance system security. Some of these configurations might be things to consider, depending on your organization.

System Preferences Overview

Mac OS X includes many system preferences that you can customize to improve 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 any of the individual preferences to view them.



Some of the more critical preferences require that you authenticate before you can modify their settings. To authenticate, you click a lock 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 secure system preference" in Security preferences. For more information, see "Securing Security Preferences" on page 85. If you log in as a standard user, these preferences remain locked. After unlocking preferences, you can lock them again by clicking the lock.



Preferences that require authentication include the following:

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

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

Securing .Mac Preferences

.Mac is a suite of Internet tools designed to help you synchronize your data and other important information for when you're away from the computer. You should not use .Mac if you must store critical data only on your local computer. You should only transfer data over a secure network connection to a secure internal server.

If you must use .Mac, enable it only for user accounts that don't have access to critical data. Do not enable .Mac for your administrator or root user accounts.

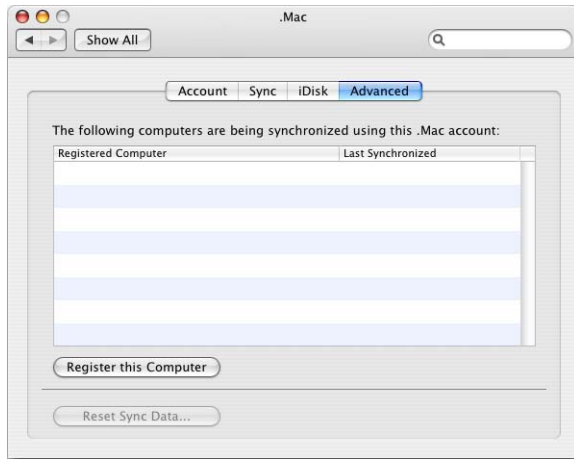
You should not enable any options in the Sync pane of .Mac preferences.



You should not enable iDisk Syncing. If you must use a Public Folder, enable password protection.



You should not register any computers for synchronization in the Advanced pane of .Mac preferences.



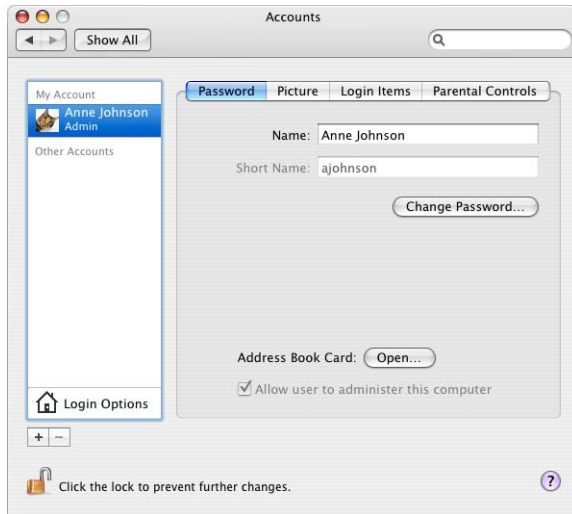
To securely configure .Mac preferences:

- 1 Open .Mac preferences.
- 2 Deselect "Synchronize with .Mac."
- 3 Don't enable iDisk Syncing in the iDisk pane.
- 4 Don't register your computer for synchronization in the Advanced pane.

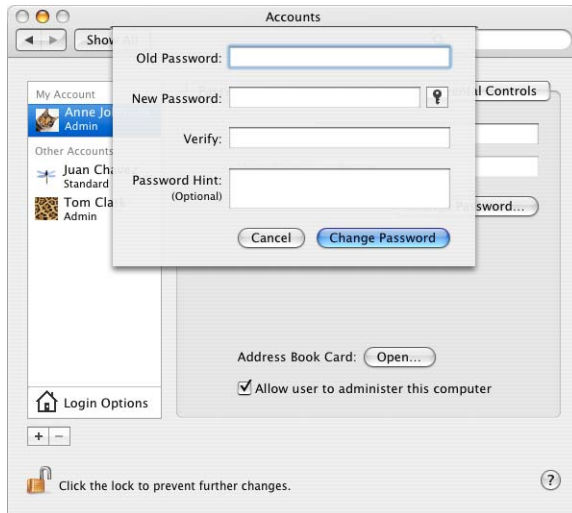
Securing Accounts Preferences

You can use Accounts preferences to perform two major security-related tasks: change or reset account passwords, and modify login options.

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

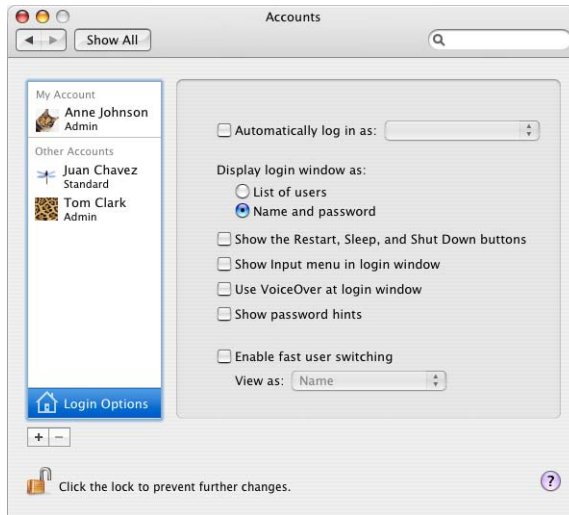


The password change and reset dialogs provide access to Password Assistant, an application that can analyze the strength of your chosen password and assist you in creating a more secure password. For information, see “Using Password Assistant” on page 51.



You should modify login options so that you provide as little information as possible to the user. You should require that the user know which account they want to log in with, and the password for that account. You shouldn't automatically log the user in, you should require that the user enter both a name and password, and that the user authenticate without the use of a password hint. Don't enable fast user switching—it is a security risk because it allows multiple users to be simultaneously logged in to the computer.

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



To securely configure Accounts preferences:

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

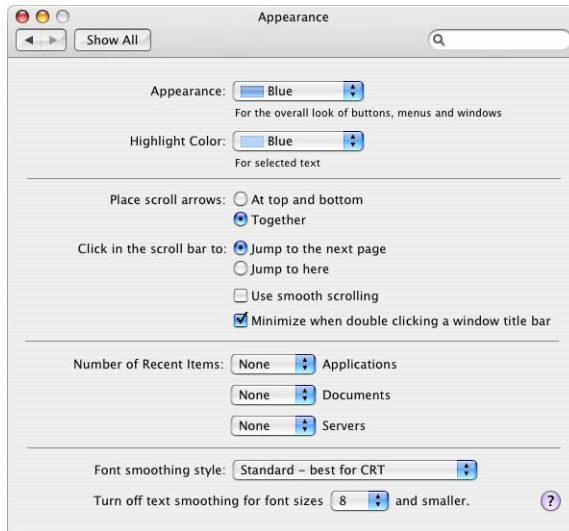
A menu will display asking you to input the old password, new password, verification of the new password, and a password hint. Do not enter a password hint, then click the Change Password button.

- 3 Click Login Options and select only "Display login window as: Name and password." Deselect all other options.

Securing Appearance Preferences

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

You should consider changing the number of recent items displayed in the Apple menu to none. 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 any authentication mechanism for servers if the corresponding keychains are unlocked. Removing recent items provides a minimal increase in security, but it can deter very unsophisticated intruders.



To securely configure Appearance preferences:

- 1 Open Appearance preferences.
- 2 Set all of the “Number of Recent Items” preferences to none.

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. You should 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. It is possible to restrict a user account's privileges so that the user cannot reenabling Bluetooth, but to do this, you also remove several important user abilities, like the user's ability to change his or her own password. For more information, see "Types of User Accounts" on page 41.



To securely configure Bluetooth preferences:

- 1 Open Bluetooth preferences.
- 2 Set Bluetooth Power to Off.

Securing CDs & DVDs Preferences

The computer should not perform automatic actions when the user inserts CDs or DVDs. 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 that the user cannot open System Preferences. For more information on restricting accounts, see "Securing Nonadministrator Accounts" on page 43.



To securely configure CDs & DVDs preferences:

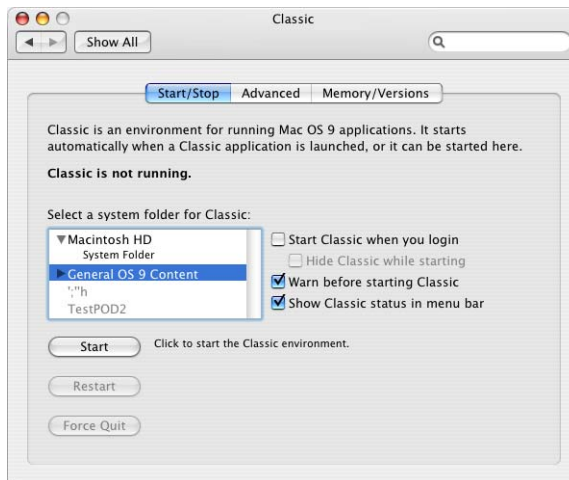
- 1 Open CDs & DVDs preferences.
- 2 Choose Ignore for each pop-up menu to disable automatic actions when inserting media.

Securing Classic Preferences

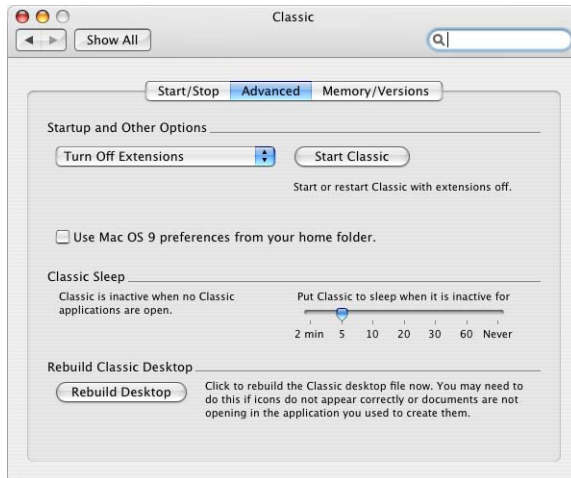
Mac OS X includes an adaptation of Mac OS 9, known as Classic. Mac OS 9 should be removed from the computer. If you remove Mac OS 9 and do not plan on using it, you do not need to configure Classic preferences. For instructions on how to remove Mac OS 9, see “Removing Mac OS 9” on page 33.

If you are going to use Mac OS 9 from a CD, DVD, or disk image, you must configure Classic preferences. Although Mac OS 9 has security issues that you cannot prevent, you can minimize Mac OS 9 security risks. For instruction, see “Running Mac OS 9 from a Disc Image” on page 34.

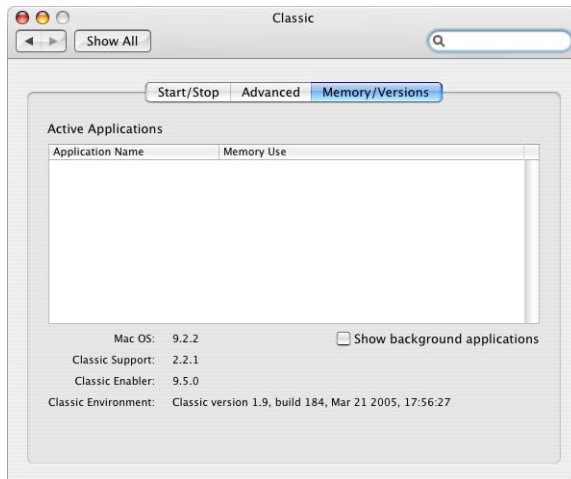
In the Start/Stop pane of Classic preferences, do not set Classic to start when you log in, and do not set Classic to hide while starting. Mac OS X should also warn before starting Classic, and show Classic status in the menu bar. By changing these settings, you increase awareness when running Classic.



Turn off extensions in the Advanced pane of Classic preferences. Although Classic is not allowed to interact directly with hardware, you might have several extensions that are related to hardware and are therefore unnecessary.



You can also use the Memory/Versions pane of Classic preferences to view the applications running in Mac OS 9. By choosing to show background applications, you become more aware of any malicious applications running in Mac OS 9.

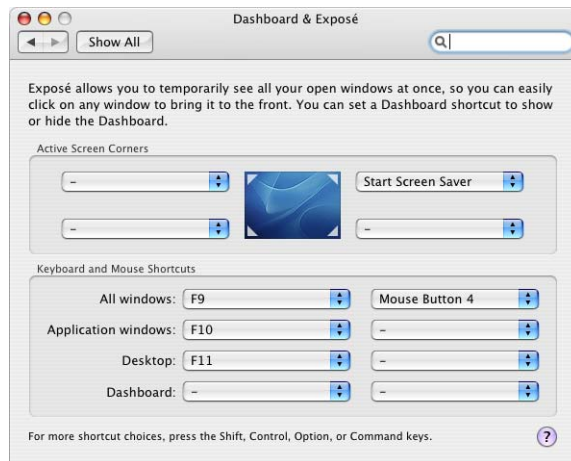


To securely configure Classic preferences:

- 1 Open Classic preferences.
- 2 In the Start/Stop pane, deselect “Start Classic when you login” and “Hide Classic while starting.”
- 3 Select “Warn before starting Classic.”
- 4 Click the Advanced pane, and select “Turn Off Extensions.”

Securing Dashboard and Exposé Preferences

Your computer should require authentication when waking from sleep or screen saver. You can configure Dashboard & Exposé preferences to allow you to quickly start the screen saver if you move your mouse cursor to a corner of the screen. You should not configure any corner to disable the screen saver.



For information about requiring authentication for the screen saver, see “Securing Security Preferences” on page 85.

The Dashboard widgets included with Mac OS X can be trusted. However, you should be careful when you install third-party Dashboard widgets. You can install Dashboard widgets without having to authenticate. If you want to prevent Dashboard, from running, set the keyboard and mouse shortcuts to “-.”

When you configure Dashboard and Exposé preferences, you must configure these preferences for every user account on the computer. This does not prevent users from reconfiguring their preferences. It is possible to restrict a user account’s privileges so that the user cannot reconfigure preferences. To do this, you will also remove several important user abilities, like the user’s ability to change his or her own password. For more information, see “Types of User Accounts” on page 41.

If your organization does not want to use Dashboard because of its potential security risk, you can disable it.

To disable Dashboard from command line:

1 Open Terminal.

2 Enter the command:

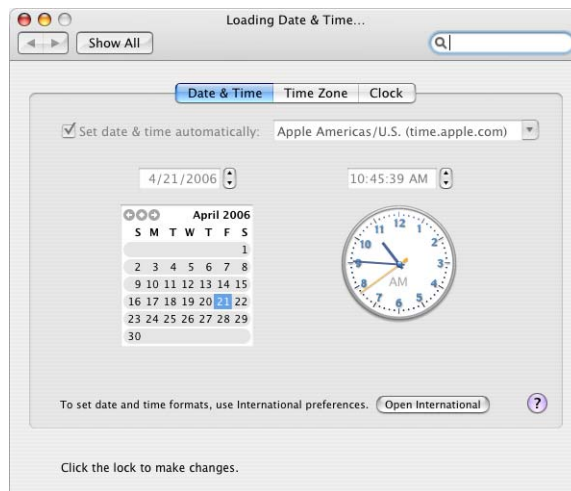
```
$ defaults write com.apple.dashboard mcx-disabled -boolean YES
```

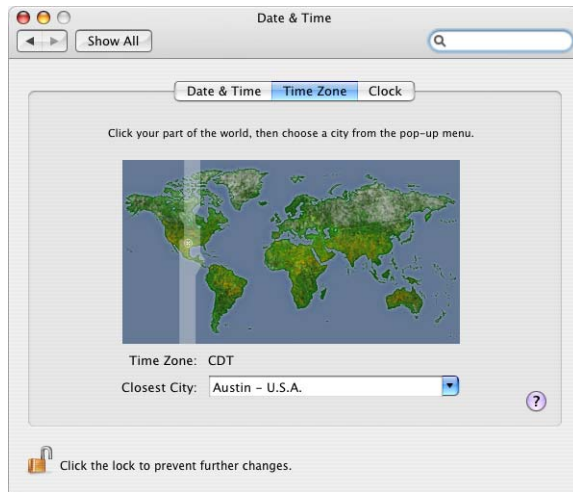
This prevents Dashboard from opening.

3 Quit Terminal.

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. Date & Time preferences can automatically set the date and time based on a Network Time Protocol (NTP) server. If you require automatic date and time, use a trusted, internal NTP server.



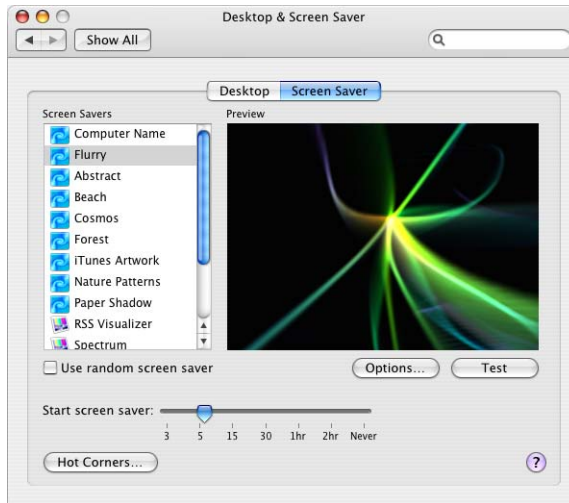


To securely configure Date & Time preferences:

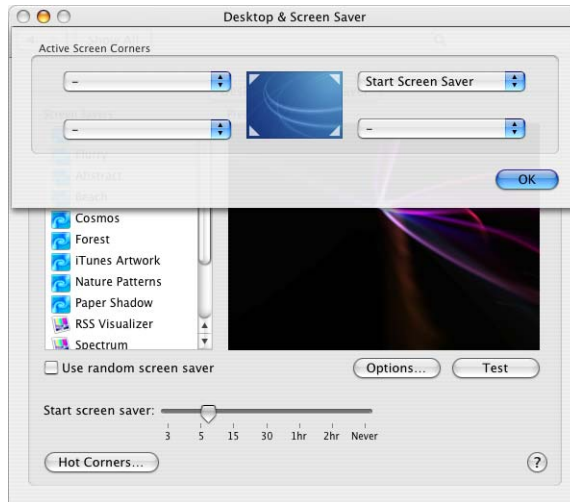
- 1 Open Date & Time preferences.
- 2 In the Date & Time pane, enter a secure and trusted NTP server in the “Set date & time automatically” field. Click the Time Zone pane.
- 3 In the Time Zone pane, choose a time zone.

Securing Desktop & Screen Saver Preferences

You can configure a password-protected screen saver to help prevent accessing of unattended computers by unauthorized users. Different authentication methods can be used to unlock the screen saver, which include digital tokens, smart cards, or biometric readers. You should set a short inactivity interval to decrease the amount of time the unattended computer spends unlocked. For information about requiring authentication for screen savers, see “Securing Security Preferences” on page 85.



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. You should not configure any corner to disable screen savers. You can also do this by configuring Dashboard & Exposé preferences.



When you configure Desktop & Screen Saver preferences, you must configure these preferences for every user account on the computer. This doesn't prevent users from reconfiguring their preferences. It is possible to restrict a user account's privileges so that the user cannot reconfigure preferences. Doing this removes several important user abilities, like the user's ability to change his or her own password. For more information, see "Types of User Accounts" on page 41.

To securely configure Desktop & Screen Saver preferences:

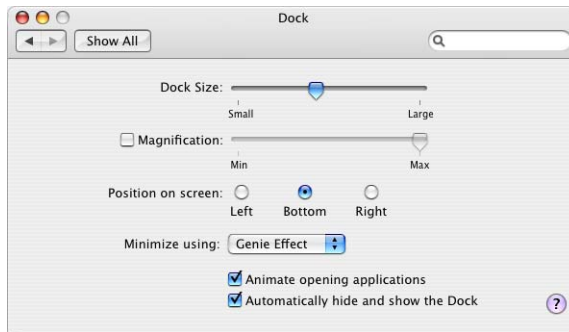
- 1 Open Desktop & Screen Saver preferences.
- 2 Click the Screen Saver pane.
- 3 Set "Start screen saver" to a short inactivity time.
- 4 Click Hot Corners.
- 5 Set a corner to Start Screen Saver for quick enabling of the screen saver.
Don't set any screen corner to Disable Screen Saver.

Securing Displays Preferences

If you have multiple displays attached to your computer, be aware that enabling display mirroring might inadvertently 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 what applications you have available on your computer when they pass by.



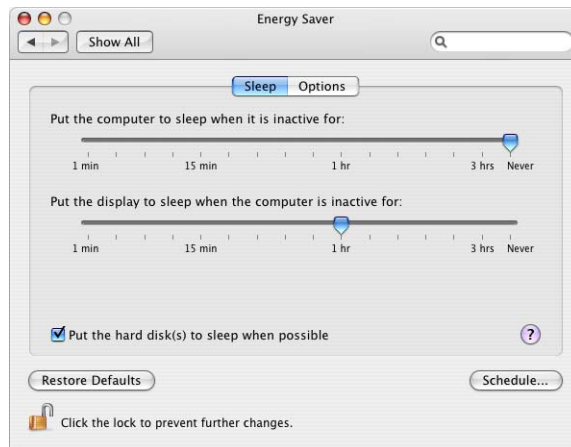
To securely configure Dock preferences:

- 1 Open Dock preferences.
- 2 Select “Automatically hide and show the Dock.”

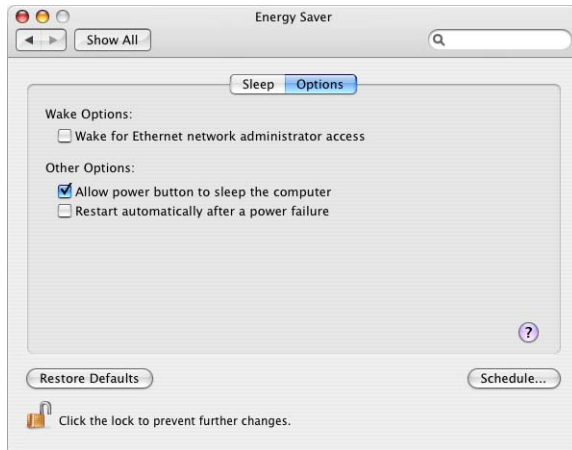
Securing Energy Saver Preferences

You can configure the period of inactivity required before a computer, display, or hard disk enters sleep mode, and require authentication by use of a password, digital token, smart card, or biometric reader when a user tries to use the computer. This is similar to using a password-protected screen saver. Mac OS X also allows you to set up different settings, depending on your power supply (power adapter or battery). For information about how to set up password protection for sleep mode, see “Securing Security Preferences” on page 85.

If the computer will be receiving directory services from a network that manages its client computers, be aware that when the computer is in sleep mode, it is unmanaged. It also cannot be detected as being connected to the network. If you want to allow management and network visibility, you can configure the display and the hard disk to sleep, but not the computer.



You should configure the computer so that it only wakes from sleep mode when you try to physically access the computer. Also, the computer should not be set to restart after a power failure.



To securely configure Energy Saver preferences:

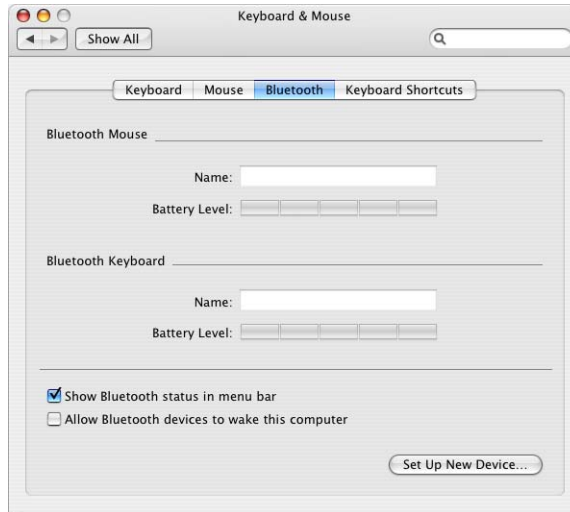
- 1 Open Energy Saver preferences.
- 2 Click the Sleep pane.
- 3 Set “Put the computer to sleep when it is inactive for:” to Never.
- 4 Select “Put the hard drive disk(s) to sleep when possible.” Click the “Options” pane.
- 5 Click the Options pane, and deselect both “Wake from Ethernet network administrator access” and “Restart automatically after a power failure.”

Securing International Preferences

No security-related configuration is necessary. However, if your computer uses more than one language, check the security risk of the language character set. It is recommended that you deselect any unused packages during the installation of Mac OS X.

Securing Keyboard & Mouse Preferences

It is recommended that Bluetooth be turned off if not required. If Bluetooth is necessary it is good practice to disable allowing Bluetooth devices to awake the computer.

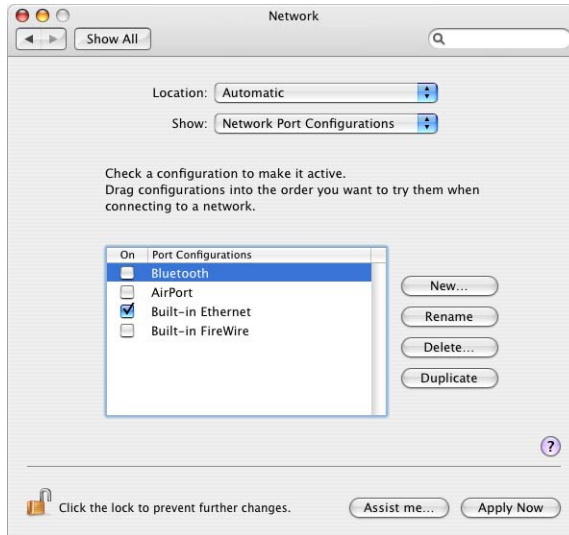


To securely configure Keyboard & Mouse preferences:

- 1 Open Keyboard & Mouse preferences.
- 2 Click Bluetooth.
- 3 Deselect "Allow Bluetooth devices to wake this computer."

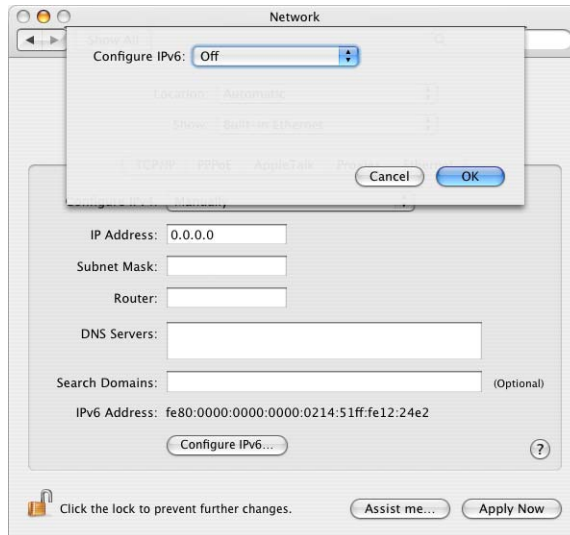
Securing Network Preferences

You should disable any unused hardware devices listed in Network preferences. 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.



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 huge number of addresses, even with the inefficiency of address assignment. 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 the vast majority of computers that use IPv6. If your organization's network is not capable of using or require IPv6, you should turn it off. You can also configure IPv6 manually.

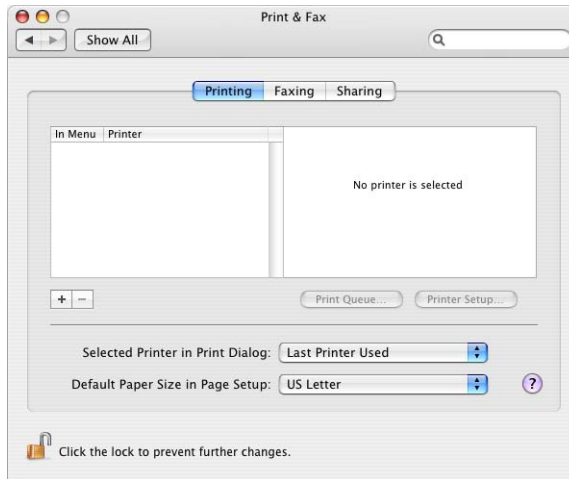


To securely configure Network preferences:

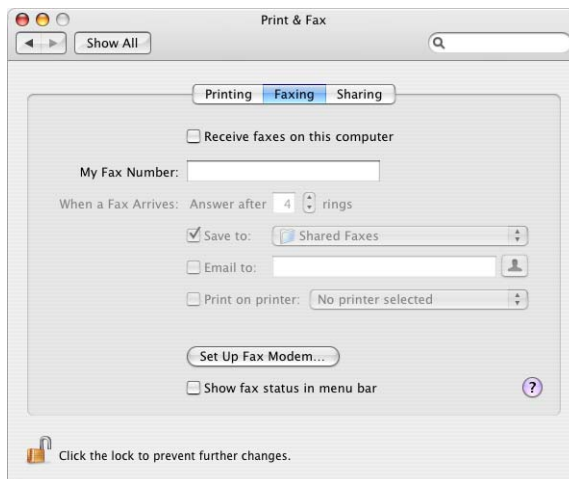
- 1 Open Network preferences.
- 2 In the Show pop-up menu, choose your network device.
- 3 Click Configure IPv6.
- 4 In the Configure IPv6 pop-up menu, choose Off.
- 5 Click OK.
- 6 In the Show pop-up menu, choose Network Port Configurations.
- 7 Deselect any unused devices to disable them.

Securing Print & Fax Preferences

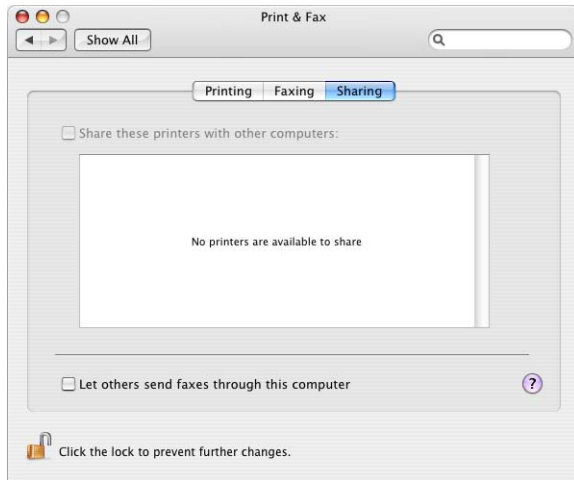
You should only use printers that are in a secure location. If you print confidential material in an insecure location, your confidential data sent to the printer might be viewable by unauthorized users. You should also be careful not to print to a shared printer, since that allows another computer to capture the complete print job directly. The remote computer could be maliciously monitoring and capturing confidential data being sent to the real printer.



You should not receive faxes on your computer. By enabling faxes, you provide an additional avenue for possible attack.



You should not use your computer to share a printer, or to send faxes. If you share a printer, unauthorized users can add items to your print queue without having to authenticate. If you enable these functions, you provide a mechanism for intruders to access your computer.

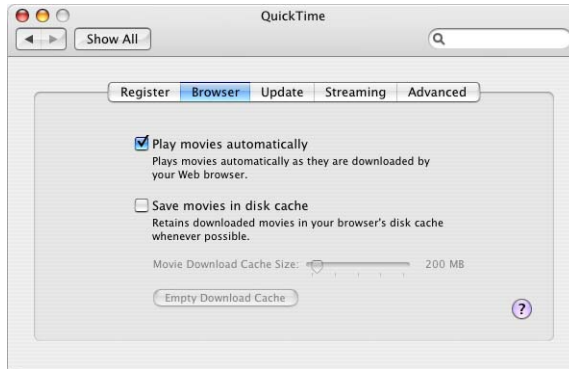


To securely configure Print & Fax preferences:

- 1 Open Print & Fax preferences.
- 2 In the Faxing pane, deselect "Receive faxes on this computer."
- 3 In the Sharing pane, deselect "Share these printers with other computers."

Securing QuickTime Preferences

You should only download QuickTime movies from trusted, secure sources. By default, QuickTime stores downloaded movies in a cache. If someone gained access to your account, they would be able to see your previously viewed movies, even if you did not explicitly save them as files. You can change QuickTime preferences to disable the storing of movies in a cache.



You should not install third-party QuickTime software unless you specifically require that software.



To securely configure QuickTime preferences:

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

Securing Security Preferences

The settings in Security preferences cover a wide range of Mac OS X security issues.

Mac OS X includes FileVault, which encrypts the information in your home folder. FileVault uses the latest government-approved encryption standard, the Advanced Encryption Standard with 128-bit keys (AES-128). For more information about FileVault, see “Encrypting Home Folders” on page 104.

You should require a password to wake the computer from sleep or screen saver. This helps prevent unauthorized access to unattended computers. Although there is a lock button for Security preferences, individual users don’t need to be authorized as an administrator to change this setting. You should enable this setting for every user account on the computer.

The settings listed under “For all accounts on this computer” require you to unlock Security preferences. You should disable automatic login, require a password to unlock Security preferences, disable automatic logout because of inactivity, and use secure virtual memory.

Disabling automatic login is necessary for any level of security. If you enable automatic login, an intruder can automatically log in without having to authenticate. Even if you automatically log in with a very restricted user account, this makes it much easier to perform malicious actions on the computer.

Some system preferences are automatically 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.

Although you might want to enable automatic logout based on inactivity, there are several reasons why you should disable this feature. First, automatic logout can disrupt your workflow. Second, automatic logout can close applications or processes without your approval (whereas a password-protected screensaver will not close applications). Third, applications can prevent successful automatic logout. For example, if you edit a file in a text editor, the text editor might ask you if you want to save the file before you can log out. Since automatic logout can be interrupted, it provides a false sense of security.

Virtual memory decreases the need for large amounts of physical memory. A swap file is used to store inactive physical memory contents, freeing up your physical memory. By default, the swap file is in an unencrypted, insecure format. This swap file can contain highly confidential data, such as documents and passwords. By using secure virtual memory, you secure the swap file at a cost of slower speed (to access the secure swap file, Mac OS X must encrypt or decrypt the secure swap file).

If you are not using the remote control, it is recommended that you disable the infrared receiver. This eliminates unauthorized users from controlling your computer through the infrared receiver.



To securely configure Security preferences:

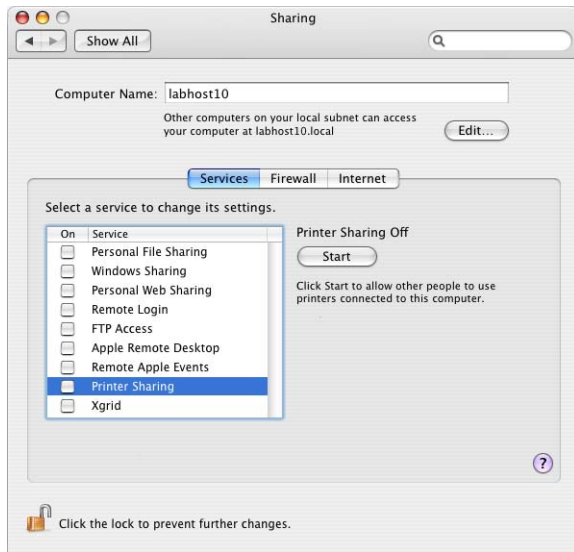
- 1 Open Security preferences.
- 2 Select “Require password to wake this computer from sleep or screen saver.”
- 3 Select “Disable automatic login.”
- 4 Select “Require password to unlock each secure system preference.”
- 5 Deselect “Log out after # minutes of inactivity.”
- 6 Select “Use secure virtual memory.”
- 7 Select “Disable remote control infrared receiver.”
- 8 Click “Turn On FileVault.”
- 9 Authenticate with your account password.

- 10 Select “Use secure erase.”
- 11 Click “Turn On FileVault.”
- 12 Restart the computer.

Securing Sharing Preferences

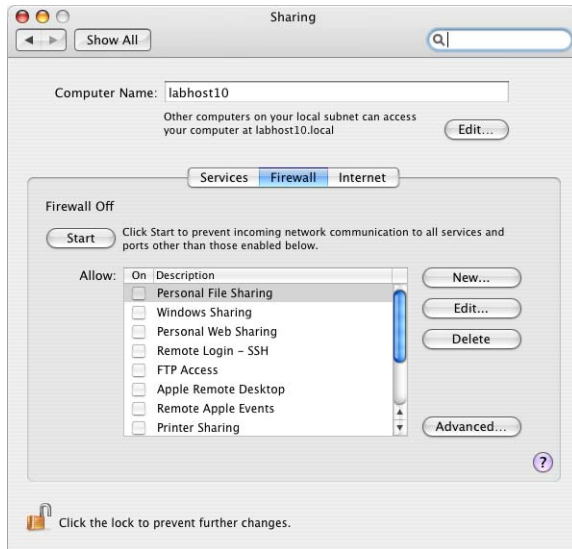
By default, every service listed in Sharing preferences is disabled. You should not enable any of these services unless you are required to use them. The following services are described in greater detail in “Securing Network Services” on page 127.

Service	Description
Personal File Sharing	Gives users of other computers access to each user’s Public folder.
Windows Sharing	Allows users to access shared files and printer using the SMB/CIFS protocol. You should disable this service. There are several well-known risks associated with SMB/CIFS.
Personal Web Sharing	Allows any user on the network to view web sites located in /Sites. If you are enabling this service, you should 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.
FTP Access	Allows users on other computers to access the computer through the File Transfer Protocol (FTP). FTP transmits passwords insecurely, in clear text. Instead, if you enabled Remote Login, you can use <code>scp</code> or <code>sftp</code> to transfer files.
Apple Remote Desktop	Allows the computer to be accessed using Apple Remote Desktop.
Remote Apple Events	Allows the computer to receive Apple events from other computers.
Printer Sharing	Allows other computers to access a printer connected to this computer.
Xgrid	Allows computers on a network to work together in a grid to process a job.

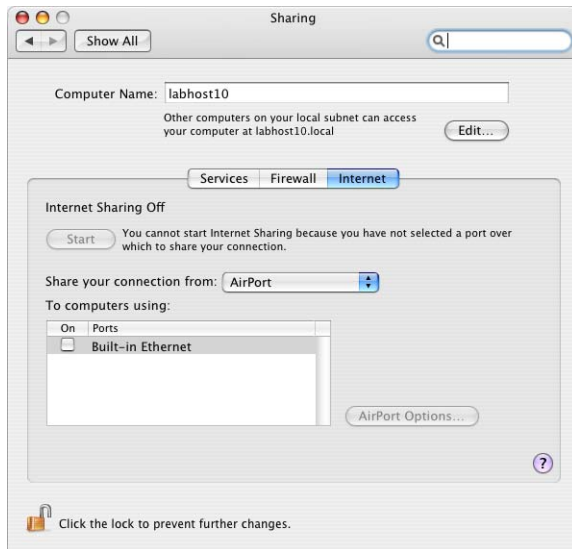


You can change your computer's name in Sharing preferences. By default your computer's host name is typically *firstname-lastname-computer*, where *firstname* and *lastname* is the system administrator's first name and last name, respectively, and *computer* is either the type of computer or simply "Computer." When other users use Bonjour to discover your available services, your computer is displayed as *hostname.local*. To increase your privacy, you should change your computer's host name so that you are not identified as the owner of your computer.

You can use the Firewall pane of Sharing preferences to enable a firewall that can block both TCP and UDP ports for any of the services listed. This firewall is very powerful and includes logging and stealth mode features.



You can use the Internet pane of Sharing preferences to disable Internet Sharing.



For more information about these services and the firewall and sharing capabilities of Mac OS X, see Chapter 7, "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.
- 3 Click the Firewall pane, and select a service you want to allowed through the firewall.
- 4 Click the Internet pane, and disable Internet Sharing.

Securing Software Update Preferences

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

Instead of using Software Update, you can also manually update your computer by using installer packages. You could install and verify updates on a test-bed 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 27.

After transferring installer packages to your computer, you should verify the authenticity of the installer packages. For more information, see "Repairing Disk Permissions" on page 28.

When you try to install a software update, either by using Software Update or by using an installer package, you are required to 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.

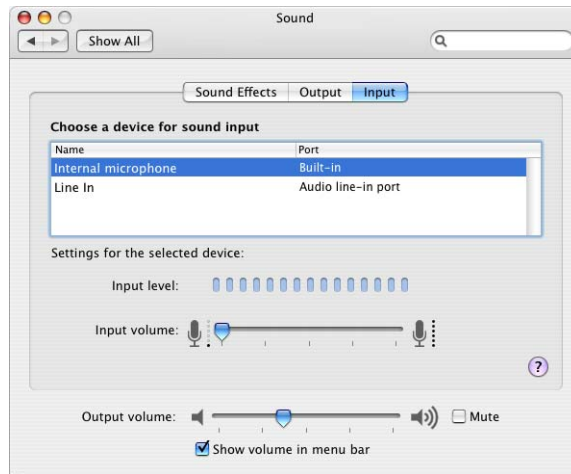


To securely configure Software Updates preferences:

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

Securing Sound Preferences

Many Apple computers include an internal microphone, which can cause security issues. You can use Sound preferences to disable the internal microphone and the line-in port.



To securely configure Sound preferences:

- 1 Open Sound preferences.
- 2 Select Internal microphone (if present), and set the “Input volume” to zero.
- 3 Select Line-In (if present), and set the “Input volume” to zero.
- 4 This ensures that “Line-In” is the devices selected rather than the internal microphone when preferences is closed, providing protection against inadvertent use of the internal microphone.
- 5 Set “Input volume” to zero.

Securing Speech Preferences

Mac OS X includes speech recognition and text to speech features, which are disabled by default. You should only enable these features if you're working in a secure environment where no one else can hear you speak to the computer, or hear the computer speak to you. Also make sure there are no audio recording devices that can record your communication with the computer.



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



To securely configure 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.

Securing Spotlight Preferences

Spotlight is a new feature in Mac OS X version 10.4. You can use Spotlight to search your entire computer for files. Spotlight searches not only the name and meta-information associated with each file, but also the contents of each file. Spotlight nullifies the use of file placement as an additional layer of security. You must still properly set access permissions on folders containing confidential files. For more information about access permissions, see “Repairing Disk Permissions” on page 28.



By placing specific folders or disks in the Privacy pane, you can prevent Spotlight from searching them. You should disable searching of all 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 individual 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 any 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.

You can use the `mdutil` tool to turn spotlight indexing off for a volume. For example, to erase the current meta store and turn indexing off for a volume called *volumename*:

```
$ mdutil -E -i off volumename
```

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

Securing Startup Disk Preferences

You can use Startup Disk preferences 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 will start up from the FireWire drive plugged into the current FireWire port for that volume. If you connect a new, different FireWire drive to that FireWire port, your computer will start from the first valid Mac OS X volume available to the computer. This is assuming you have not enabled the Open Firmware password.

When you enable an Open Firmware password, the FireWire volume you selected is the only volume that will start the computer. Open Firmware locks in the FireWire Bridge Chip GUID as a startup volume instead of the hard drive's GUID (as is done with internal hard drives). If the drive inside the FireWire drive enclosure is replaced by a new drive, the computer can start from the new drive without having to bypass the Open Firmware password. To avoid this type of intrusion, make sure your hardware is physically secured. Open 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 31.



You can also restart in target disk mode from Startup Disk preferences. When your computer is in target disk mode, another computer can connect your computer and access your computer's hard drive. The other computer has full access to all the files on your computer. All file permissions for your computer are disabled in target disk mode.

If you hold down the T key during startup, you enter target disk mode. You can prevent the startup shortcut for target disk mode by enabling an Open Firmware or EFI password. If you enable an Open Firmware or EFI password, you can still restart in target disk mode using Startup Disk preferences. For more information about enabling an Open Firmware or EFI password, see “Using the Open Firmware Password Application” on page 36.

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.

Securing Universal Access Preferences

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

- See the device manual for prevention of possible security risks.
- Enabling VoiceOver configures the computer to read the contents under the cursor out loud, which might inadvertently disclose confidential data.
- These devices allow access to the computer that could reveal information in a compromising manner.

Your data is the most valuable part of the computer. By using encryption, you can protect your data in the 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. Using the secure erase feature of Mac OS X, any deleted data is completely erased from the computer.

Understanding Permissions

Files and folders are protected by setting permission that restrict or allow users access to 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 in its process of verifying file and folder permissions. The process that ACL uses to determine if an action is allowed or denied includes checking specific rules called access control entries (ACEs). If none of the ACEs apply, then standard POSIX permissions are used to 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 different categories of users (owner, group, and everyone). There are four types of standard POSIX access permissions that you can assign 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 three categories of users:

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

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

To view the permissions of folders or files:

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

```
$ ls -l
```

Output similar to the following will be displayed

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

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

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

Interpreting POSIX Permissions

POSIX permissions can be interpreted by reading the first ten bits of the long format output listed for a file or folder.

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

In this example, the `NewFolder` has the POSIX permissions `drwxr-xr-x` and has an owner and group of `ajohnson`. The `d` of the POSIX permissions signifies that `newfolder` is a folder. The first three letters after the `d` (`rwX`) signify that the owner has read, write, and execute permission for that folder. The next three characters, `r-x`, signify that the group has read and execute permission. The last three characters, `r-x`, signify that all others have read and execute permission. In this example, any users who can access `ajohnson's ~/Documents/` folder can also open the `NewFolder` folder and can view, but not 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` will be able to access the folder. This is because `ajohnson's ~/Documents/` folder has `drwx----` POSIX permissions.

By default, most of the user's folders have `drwx-----` POSIX permissions. Only the `~/Sites/` and `~/Public/` folders have `drwxr-xr-x` permissions. This set of permissions allows other people to view folder contents without authenticating. You can change these folder permissions to `drwx-----` if you do not want other people to view their contents. Within the `~/Public/` folder, the Drop Box folder has `drwx-wx-wx` POSIX permission. This allows users other than `ajohnson` to add files into a `ajohnson's drop box` but they are not able to view those files.

Occasionally, you'll see a `t` instead of an `x` 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 is something that can become common if several people are granted `rwX` access. The sticky bit being set 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.

See the `sticky` man page for more information.

Modifying POSIX Permissions

After you determine the current POSIX permission settings, you can modify them by using the `chmod` command.

To modify POSIX permission:

- 1 Enter the following in Terminal.

```
$ chmod g+w file.txt
```

This adds write permission for the group to `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 ajohnson   68 Apr 28 2006 NewFolder
-rw-rw-r-- 1 ajohnson ajohnson 43008 Apr 14 2006 file.txt
```

For more information, see the `chmod` man page.

Setting File and Folder Flags

Files and folders can also be protected using flags. These flags, or permission extensions, override standard POSIX permissions. These can be used to prevent the system administrator (root) from modifying or deleting files or folders.

Use the `chflags` command to enable and disable flags. The flag can only be set or unset by the file's owner or an administrator using `sudo`.

Viewing Flags

Before setting or changing file or folder flags, you should 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
```

In this example the flag settings for a folder named `secret` are displayed.

Modifying Flags

After you determine the current file or folder flag settings, you can modify them using the `chflags` command.

To lock a folder using flags:

```
$ sudo chflags uchg secret
```

In this example, the folder named `secret` is locked. To unlock the folder, change `uchg` to `nouchg`.

```
$ sudo chflags nouchg secret
```

WARNING: There is an `schg` option for the `chflags` command. It sets the system immutable flag. This setting can only be undone when the computer is in single-user mode. If this is done on a RAID, XSan, or other storage that cannot be mounted in single user mode, the only way to undo the setting is to reformat the RAID or XSan.

For more information, see the `chflags` man page.

Setting ACL Permissions

For greater flexibility in configuring and managing file permissions, Mac OS X implements access control lists (ACL). An ACL is an ordered list of rules that control file permissions. Each rule or access control entry (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 how these permissions are propagated throughout a folder hierarchy.

ACLs in Mac OS X let you set file and folder access permissions for multiple users and groups, in addition to the 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 and Windows XP.

To determine if an action is allowed or denied, the 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 none of the ACEs apply, then standard POSIX permissions determine access.

Enabling ACL

By default, ACLs are not enabled in Mac OS X. The volume must be enabled to support ACLs. The following example uses the `fsaclctl` command to enable ACLs on a Mac OS X startup volume:

```
$ sudo /usr/sbin/fsaclctl -p / -e
```

For more information, enter `fsaclctl` in a Terminal window.

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 a specific 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 a 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.

Setting Global File Permissions

Every file or folder has POSIX permissions associated with it. When you create a new file or folder, the `umask` setting determines these POSIX permissions. The default `umask` setting `022` (in hexadecimal), removes group and other write permissions. Group members and other users can read and run these files or folders. If you change this `umask` setting to `027`, files and folders can still be read and run by group members, but cannot be accessed in any way by others. If you want to be the only user who can access your files and folders, set the `umask` setting to `077`.

To change the globally defined `umask` setting, change the `NSUmask` setting. However, not all applications recognize the `NSUmask` setting. Therefore, there is no guarantee that files and folders created by other applications will have proper `umask` settings. The `NSUmask` setting also doesn't affect some command-line tools.

To change the global umask:

- 1 Open Terminal.
- 2 Change the NSUmask setting to be the decimal equivalent of the umask setting:

```
$ sudo defaults write /Library/Preferences/.GlobalPreferences NSUmask 23
```

You must be logged in as a user who can use `sudo` to perform these operations.

This example sets the global umask to 027, which has the decimal equivalent of 23.

Replace `23` with the decimal equivalent of your desired umask setting. This command requires that you use the decimal equivalent, and not a hexadecimal number.

Important: Make sure the path you enter is `.GlobalPreferences`—not `.GlobalPreferences.plist`, which might be accidentally added by Terminal's autocompletion feature.

- 3 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 individual files and folders.

Securing Your Home Folder

Change the permissions of each user's home folder so that they are no longer world-readable or world-searchable. When FileVault is not enabled, the permissions on the home folder of a newly-created user account allow any other user to browse its contents. The `~/Public` and `~/Public/Drop Box` folders within each home folder require these permissions. However, users may inadvertently save sensitive files directly into their home folder, instead of into the more-protected `~/Documents`, `~/Library`, or `~/Desktop` folders. Although `~/Public` and `~/Public/Drop Box` folders will no longer work as intended, the permissions on each user's home folder should be changed to prevent other users from browsing its contents.

Enter the following command to change home folder permissions:

```
$ sudo chmod 750 /Users/username
```

Replace *username* with the name of the account.

Run this command immediately after everytime someone creates a new account. The 750 permission setting still allows members of the group owning the folder to browse it, but in Mac OS X version 10.3 or later that group consists only of the user. If more advanced group management is performed and members of the group owning the folder should not be granted permission to browse it, then the command above should be issued with the permission 700 instead of 750. The user, as the owner of his home folder, can alter its 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 all the files contained within it. You should use FileVault on portable computers, and on any other computers whose physical security you cannot guarantee. You should enable FileVault encryption for your computer and for all its user accounts.

FileVault moves all the content of your home folder into a sparse disk image that uses AES-128 encryption. The sparse format allows the image to maintain a size proportional to its contents, which can save disk space.

If you remove files from a FileVault-protected home folder, it takes some time to recover free space from the home folder. Once 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 having to recover free space. For more information, see "Encrypting Portable Files" on page 105.

If you've insecurely deleted files before using FileVault, these files are still recoverable after activating it. When initially enabling FileVault, securely erase free space. For information, see "Using Disk Utility to Securely Erase Free Space" on page 111.

FileVault does not encrypt or protect files transferred over the network or saved to removable media, so you'll want to encrypt specific files or folders. If you mount these encrypted images, all data transmitted over the network will be encrypted with AES-128. For information about encrypting specific files or folders for transfer from your network home folder, see "Encrypting Portable Files" on page 105.

To 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 both your login password and your master password, you will not be able to recover your data. Consider sealing your master password in an envelope and storing it in a secure location. You can also use Password Assistant to help create a complex master password that cannot be easily compromised. For information, see "Using Password Assistant" on page 51 and "Creating Complex Passwords" on page 149.

Enabling FileVault copies all 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 you have the option of using secure erase. Enable secure erase, so that your unencrypted data is securely erased.

Using FileVault Master Keychain

A FileVault master keychain can be set to decrypt any account using FileVault to encrypt data. It is recommended that FileVault keychain be set to ensure data is not lost in the event of a forgotten password. If a user forgets their FileVault account password, which is used to decrypt their encrypted data, the FileVault master keychain can be used to decrypt the data.

To create the FileVault master keychain:

- 1 Open System Preferences > Security.
- 2 Click Master Password and set a master password.

Select a very strong password and consider splitting the password into at least two components (first half and second half). Using Password Assistant can ensure that the quality of the password selected is strong. Each password component would be kept by separate security administrators, to avoid one person knowing the full password. This prevents a single person from unlocking (decrypting) a FileVault account, by requiring two or more security administrators. For more information, see “Using Password Assistant” on page 51.

This creates a keychain called FileVaultMaster.keychain in /Library/Keychains/. The FileVault master keychain now contains both a FileVault recovery key (self-signed root CA Certificate) and a FileVault master password key (private key).

- 3 You can delete the corresponding certificate called 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 corresponding private key, so there is no security concern with anyone gaining access to this certificate.

- 4 Make a copy of the FileVaultMaster.keychain and put it in a secure place.
- 5 Delete the private key from FileVaultMaster.keychain created on the computer to modify the keychain.

This ensures that even if someone is able to unlock the FileVault master keychain, they are unable to decrypt the contents of a FileVault account since there is no FileVault master password private key available for the decryption.

Encrypting Portable Files

To protect files that you want to transfer over a network or save to removable media, you should either encrypt a disk image or encrypt the individual 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 all network traffic between the computer and the server hosting the mounted encrypted disk image.

Creating a New Encrypted Disk Image

You can create a read/write image or a sparse image to encrypt and securely store data. A read/write image consumes the entire 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, then that image will consume 10 GB of space even if it contains only 2 GB of data. A sparse image will only consume the amount of space of the data contained in the image. For example, if the maximum size of a sparse image is 10 GB and the data contained in it is only 2 GB, it will consume only 2 GB of space.

If you are in a situation where it is possible to have unauthorized administrator access to your computer, creating an encrypted blank disk image is preferable to creating an encrypted disk image from existing data.

Creating an encrypted image from existing data copies the data from an unprotected area into the encrypted image. If the data is sensitive it is better to create the image prior to creating the documents, since the working copies, backups, or caches of files would all be created in the encrypted storage from the start.

To create a new encrypted disk image:

- 1 Open Disk Utility.
- 2 Choose File > New > Blank Disk Image.
- 3 Enter a name for the image and choose where to store it.
- 4 Choose the size of the image by clicking the Size pop-up menu.
You cannot increase the size of an image after creating it. Make sure that the size of the image is large enough for your needs.
- 5 Choose an encryption method by clicking the Encryption pop-up menu.
AES-128 is a strong encryption format.
- 6 Choose a format by clicking the Format pop-up menu.
Although there is some overhead, the sparse format allows the image to maintain a size proportional to its contents (up to its maximum size), which can save disk space.
- 7 Click Create.
- 8 Enter a new password and verify it.
You can easily access Password Assistant from this window. For more information, see “Using Password Assistant” on page 51.
- 9 Deselect “Remember password (add to Keychain).” 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 email attachments or FTP, or copying to removable media, such as a CD-R or floppy disk.

If you plan to add more files to this image later instead of creating an image from existing data, create a new encrypted disk image and add your existing data to it. For information, see "Creating a New Encrypted Disk Image" on page 106.

To create an encrypted disk image from existing data:

- 1 Open Disk Utility.
- 2 Choose File > New > Disk Image from Folder.
- 3 Select a folder, and click Image.
- 4 Choose File > New > Blank Disk Image.
- 5 Enter a name for the image and choose where to store it.
- 6 Choose a format by clicking the Format pop-up menu.
The compressed disk image format can help you save hard disk space by reducing your disk image size.
- 7 Choose an encryption method by clicking the Encryption pop-up menu.
AES-128 is a strong encryption algorithm.
- 8 Click Save.
- 9 Enter a new password and verify it.
You can easily access Password Assistant from this window. For more information, see "Using Password Assistant" on page 51.
- 10 Deselect "Remember password (add to Keychain)." Click OK.

Creating Encrypted PDFs

You can quickly create encrypted, read-only PDF documents of confidential or personal data. To open these files, you must know the password for the PDF file.

Note: Some applications do not support printing to PDF. In this case, create an encrypted disc image. For information, see "Creating an Encrypted Disk Image from Existing Data" on page 107.

To create an encrypted, 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 Encrypt PDF.
- 4 Enter a password and verify it. Click Continue.
- 5 Enter a name for the document and choose a location. Click Save.

You should test your document by opening it. You'll be required to enter the password before you can view the contents of your document.

Securely Erasing Data

When you erase a file, you're actually just removing information that tells the file system where to find the file. The file's location on the disk is marked as free space. It is still possible to get this data from the disk if other files have not been written over the free space.

Mac OS X provides several ways to securely erase files. You'll have the choice of using one of three erase methods: a zero-out erase, a 7-pass erase, or a 35-pass erase. A zero-out erase sets all data bits on the disk to 0, while 7-pass and 35-pass use algorithms of varying complexity to overwrite the disk. 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

Note: 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.

Using Disk Utility to Securely Erase a Disk or Partition

You can use Disk Utility to securely erase a partition, using any of three methods: 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 have to use your installation discs. In the Finder, open Disk Utility (located in /Applications/Utilities/).

WARNING: Securely erasing a partition is irreversible. Be sure to back up any critical files that you want to keep before erasing the partition.

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 will start up from the disc in the optical drive.
- 3 Proceed past the language selection step.
- 4 Choose Utilities > Disk Utility.
- 5 Select the partition that you want to securely erase.
Be sure to select a partition, not a drive. Partitions are contained within 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 one of the erase options and click OK. Click Erase.
Securely erasing a partition can take a while to complete, depending on the size of the partition and the method you've chosen.

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 have the flexibility to remove each specified file or folder by overwriting, renaming, and truncating the file or folder before erasing them. This prevents other people from undeleting or recovering any information about the file or folder.

For instance, `srm` supports simple methods, like overwriting data with a single pass of zeros, to more complex ones, like using a 7-pass erase 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. Be sure to back up any critical files that you want to keep before securely erasing files.

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) only overwrites with a single random pass.

For a more secure erase, you can use the `-m` (medium) 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 quickly and securely erase all files stored in the Trash. Depending on the total size of the files being erased, securely emptying the Trash might take some time to complete.

WARNING: Using Secure Empty Trash is irreversible. Be sure to back up any critical files that you want to keep before securely erasing files.

To use Secure Empty Trash:

- 1 Open the Finder.
- 2 Choose Finder > Secure Empty Trash.
- 3 Click OK.

Using Disk Utility to Securely Erase Free Space

You can use Disk Utility to securely erase free space on partitions, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

To securely erase a free space using Disk Utility:

- 1 Open Disk Utility (located in /Applications/Utilities/).
- 2 Select the partition on which you want to securely erase free space.
Be sure to select a partition, not a drive. Partitions are contained within drives, and are indented one level in the list on the left.
- 3 Click Erase, and then click Erase Free Space.
- 4 Choose one of the erase options and click Erase Free Space.
Securely erasing free space can take a while to complete, depending on the amount of free space being erased and the method you've chosen.
- 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
```

See the `diskutil` man page for more information about how to securely erase free space.

Securely configuring network services is an important step in the process of securing your computer against network attacks.

Organizations depend on network services to communicate with other computers, both on a private network and on a wide area network. Improperly configured network services provide an avenue for attacks. This chapter recommends settings and configurations for network services, to improve the security of network communication.

Securing Apple Applications

Although Apple applications are secure by default, you can further enhance security.

Securing Mail

You can change Mail preferences to enhance security. Depending on your mail server settings, consider changing your Mail preferences so that you use SSL, and use a Kerberos-based authentication method. These settings must match those provided by your mail server. However, using these settings increases your mail security.

You should only send email that is digitally signed and encrypted. Digitally signed messages let your recipients verify your identity as the sender, and provide assurance that the message has not been 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 the desired recipients when you either already have received a digitally signed message from them or you have access to their public key. Recipients receive your public key when they receive your signed messages. This certificate-based system is commonly referred to as public key infrastructure-based (PKI) messaging. It ensures 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 automatically recognizes sender and recipient certificates. It notifies you of the inclusion of certificates by displaying a Signed (checkmark) icon and an Encrypt (closed lock) icon. When sending signed or encrypted email messages, the sender's certificate must contain the case-sensitive email address listed in Mail preferences.

You can disable the display of remote images in HTML messages in Mail's Viewing preferences. Bulk mailers can use image-tracking mechanisms to find individuals who open junk email. If you don't automatically 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."

Securing Web Browsing

You can change Safari preferences to enhance security. In particular, you should change your Safari preferences to disable all AutoFill options, opening safe files after downloading cookies (only from sites you navigate to), and ask before sending nonsecure forms.

After disabling cookies, you should remove all of your existing cookies. You can remove cookie using the Show Cookies dialog in Safari's Security preferences. For the websites that require cookies, enable cookies and then disable cookies after visiting the site. However, enabling and disabling cookies can be time consuming if you visit many sites that use cookies. Consider using multiple accounts with different cookie settings. Your personal account might allow all cookies, while your more secure account has restrictive cookie settings.

When using Safari, you should always use private browsing. Private browsing prevents Safari from logging your actions, adding webpages to the history, keeping items in the Downloads window, saving information for AutoFill, and saving your Google searches. However, you can use the Back and Forward buttons to navigate through your previously visited sites. Once you close the window, the Back and Forward history is removed.

After using Safari, you should always empty the cache. Caching improves performance and reduces network load by storing previously viewed webpages and webpage content on your local hard disk, but it is a security risk because these files are not automatically removed.

Safari supports both server-side and client-side authentication using X.509 certificates. Server-side authentication occurs when you access webpages with an "https:" URL. When Safari uses client-side authentication, it provides the server with a valid credential. This credential 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-browsing application, consider applying similar security guidelines.

For information about how to perform these tasks and for other Safari security tips, open Safari Help and search for “security.”

Securing Instant Messaging

You can use iChat to send secure text, audio, and video messages. You can also use iChat to securely send files. To set up secure iChat messaging, both you and your buddy must have a .Mac membership and have Mac OS X version 10.4.3 or later installed. With a .Mac membership, you can sign up for a Secure iChat certificate that allows you to enable secure messaging. When you enable iChat encryption, iChat performs a Certificate Signing Request (CSR) to .Mac. iChat then receives a certificate, which includes your original public key and a private key. The public and private key pair was created by the CSR process. The private key and certificate represent your .Mac identity. These keys are used for the encryption of content between you and your buddy.

When you securely send a message, iChat first 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 own private key. Although iChat is secure, messaging services allow for the possibility of an attack. Messaging services should be disabled unless your organization requires it.

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.

You should also 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 the collaboration services administration guide.

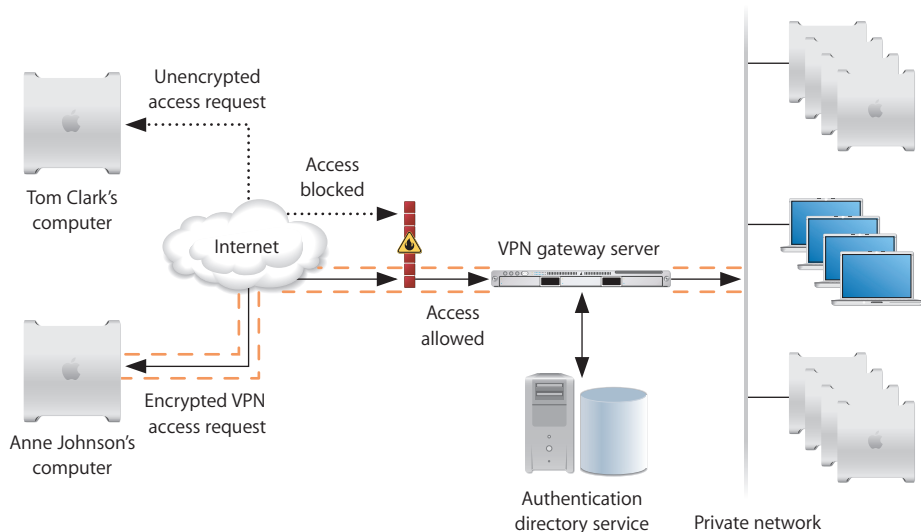
Securing VPN

Using a Virtual Private Network (VPN) is a way to have a secure, encrypted network connection while using an insecure network like the Internet. Whenever you connect to a network, you are given an IP address. With a VPN connection, you are also given a private VPN address on the internal network. Any transaction with the internal network uses VPN. Without a VPN connection, any attempt to communicate with computers inside a private network can be blocked by your organization’s firewall. If someone snoops your VPN connection, they will only see encrypted packets.

To use VPN, you connect using a transport protocol—either L2TP over IPSec or PPTP. L2TP over IPSec is more secure. PPTP provides compatibility with VPN servers that don't support L2TP over IPSec. It supports 128-bit and 40-bit encryption. 128-bit encryption is much more secure than 40-bit encryption.

VPN also requires that you authenticate both yourself and the computer. For L2TP over IPSec, you can authenticate yourself with a password, a “One-Time Password” (from a security token, provided by either RSA's SecurID or CRYPTOCard's KT-1), a certificate, a smart card, or through Kerberos. You can authenticate the computer with a shared secret (similar to a password), or a certificate. These settings should match those expected by your VPN server.

You can use Internet Connect to configure VPN access. For more information, open Internet Connect Help and search for “VPN.”



VPN allows an authorized user to connect remotely to a secure network while keeping unauthorized users out. For example, a user (Anne Johnson) can connect to her office from home by sending an encrypted VPN request to the office's VPN gateway server via the Internet. Next, the office firewall will verify that the connection is a valid encrypted VPN request and block all other unencrypted connections (Tom Clark).

Once the authorized user (Anne Johnson) is connected through the firewall, she must validate her credentials with the office VPN gateway server. If her credentials are valid, Anne Johnson is granted access to the private network and assigned a private IP address. If her credentials are not valid, access to the private network is denied.

An attacker cannot view data transferred between Anne Johnson and the office because the VPN is an encrypted connection. To ensure secure remote communication, you should use encrypted connections only.

Securing Firewall

Mac OS X includes firewall software that you can access in the Firewall pane of Sharing preferences. When you enable the firewall, the computer only allows communication on ports used by required services. You can enable or disable the following firewall ports:

- Personal File Sharing
- Windows Sharing
- Personal Web Sharing
- Remote Login - SSH
- FTP Access
- Apple Remote Desktop
- Remote Apple Events
- Printer Sharing
- iChat Bonjour
- iTunes Music Sharing
- iPhoto Bonjour Sharing
- Network Time

These ports are also enabled and disabled automatically when you turn the corresponding service on or off in the Services pane of Sharing preferences.

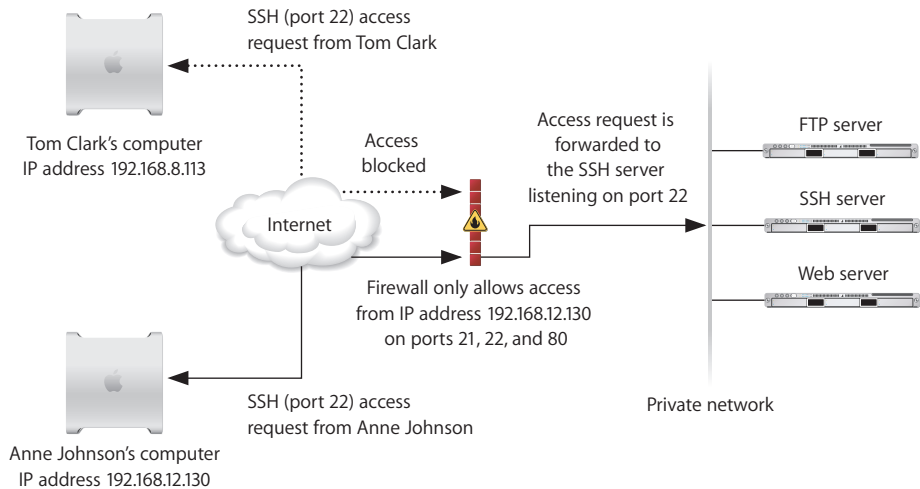
The firewall can block both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) communication, or just TCP communication. Blocking UDP traffic can help to further secure your computer.

You can enable logging of firewall activity, including blocked sources, blocked destinations, and blocked attempts.

The firewall also includes the ability to enable stealth mode. Stealth mode prevents closed ports from responding to unwanted network probes, which are typically used to acquire forensic knowledge of how to attack your computer or network. Stealth mode doesn't protect open ports. If you enable Remote Login or Personal File Sharing in Sharing preferences, the ports for those services are not protected by stealth mode.

For more information, open Mac Help and search for "firewall."

Mac OS X also includes `ipfw`, a command-line firewall tool. You can fully customize this tool and use it to set up advanced firewall rules. For information, enter `man ipfw` in a Terminal window.



Any information that is sent to a firewall is allowed or blocked based on the firewall rules:

- If a request is accepted, the firewall allows the connection through.
- If stealth mode is not enabled and a request comes in on a closed port, the firewall blocks the request and sends a reply that the connection was blocked.
- If stealth mode is enabled and a request comes in on a closed port, the firewall drops the request and does not reply.

About 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 would expose the organization's network to attack.

Enabling TCP Wrappers

A TCP wrapper is an application that can control a particular service and allow traffic from only certain computers or networks in and out of a particular port. You can use the `tcpd` command-line tool to enable a TCP wrapper.

By using TCP wrappers you can enhance the security of your network by further defining specific access to a particular service. For example, you can configure TCP wrapper to permit a user to use SSH or Web services and deny all other users access.

You can enable `tcpd` for specific command-line tools. This requires you to edit configuration files for those tools. Be careful when editing the configuration file for a tool, because an error can disable the tool. For more information, enter `man tcpd` in a Terminal window.

To enable TCP wrappers for a command-line tool:

- 1 Open Terminal.
- 2 Enter the following command:
- 3 Enter `ls` to display the contents of the folder.
- 4 Enter the following command:

```
$ cd /System/Library/LaunchDaemons/
```

```
$ sudo pico name_of_tool.plist
```

Replace `name_of_tool` with the name of the command-line tool that will use TCP wrappers. For example, `ssh.plist` is the configuration file for the `ssh` command-line tool, that can use TCP wrappers.

This command loads the tool's configuration file in the `pico` text editor. For information about how to use `pico`, enter `man pico` in a Terminal window.

- 5 Two lines below `<key>ProgramArguments</key>`, replace the text between `<string>` and `</string>` with the text between `<string>` and `</string>` in the line below `<key>Program</key>`.
- 6 In the line below `<key>Program</key>`, replace the text between `<string>` and `</string>` with:

```
/usr/libexec/tcpd
```
- 7 Save the file and exit the text editor.

Securing SSH

You can use the `ssh` command-line tool to securely connect to remote computers. The `ssh` tool enables several forms of authentication, including password and key-based authentication. It also encrypts data that travels over the network, and prevents data from being altered in transit.

Enabling an SSH Connection

You must first enable Remote Login in Sharing preferences on the server. For more information, see “Securing Sharing Preferences” on page 87.

To establish a secure SSH connection, you should 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 enable an SSH connection:

- 1 On the server and the client, open Terminal.
- 2 On the server, configure Energy Saver preferences so that the computer never goes to sleep. The hard drive can go to sleep.

For more information, see “Securing Energy Saver Preferences” on page 77.

- 3 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.

Note: When you connect to a host using the IP address, entries will be created in the `ssh_known_hosts` file. If you connect to the same host using its host name, a separate entry will be created in the `ssh_known_host` file. 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 currently logged in as, and the IP address of the server.

- 4 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.

- 5 Compare the fingerprint displayed on the client with the one displayed on the server. If they match, enter `yes` on the client. If they do not match, your connection is not authentic.

You should never have to validate the server's fingerprint again. If you are asked to validate the server's fingerprint again, your connection has been compromised. It is also possible that Mac OS X has been reinstalled on the server. Verify with the server administrator to ensure 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 be displayed in the prompt. Enter `whoami` to display your user name.
- 8 On the server and client, enter the following command:

```
$ exit
```

Configuring a Key-Based SSH Connection

By default, SSH supports the use of password, key, and Kerberos authentication.

You can modify the `ssh` command so that it only supports key-based authentication. With key-based authentication, both the client and server have public and private keys. The two computers exchange public keys. When the two computers communicate with each other, they send data 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 that key file. Password authentication can be compromised without needing a private key file.

To perform this task, you must first enable an SSH connection. For information, see "Enabling an SSH Connection" on page 120.

Note: If the server uses FileVault to encrypt the home folder of the user you want to use SSH to connect as, you have to be logged in on the server to be able 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 very 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 to enter a passphrase, enter a complex password.

A complex password is at least twelve letters long and is composed of mixed-case characters, numbers, and special characters. For more information, see “Creating Complex Passwords” on page 149.

- 6 On the client, enter the following command:

```
$ scp ~/.ssh/id_dsa.pub username@ipaddress:~/.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`.

- 7 On the client, authenticate with the password of the user whose name you entered.

- 8 On the server, enter the following command:

```
$ sudo pico /private/etc/sshd_config
```

Authenticate, if requested.

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:

Default	Replace with	Modification Notes
<code>#PermitRootLogin yes</code>	<code>PermitRootLogin no</code>	Prevents logging in as root through SSH
<code>#PasswordAuthentication yes</code>	<code>PasswordAuthentication no</code>	Disables password authentication
<code>#PermitEmptyPasswords no</code>	<code>PermitEmptyPasswords no</code>	Denies access to accounts without passwords
<code>#PubKeyAuthentication yes</code>	<code>PubKeyAuthentication yes</code>	Enables key-based authentication
<code>#RSAAuthentication yes</code>	<code>RSAAuthentication no</code>	Disables RSA authentication (not needed for key-based authentication)
<code>#RhostsRSAAuthentication no</code>	<code>RhostsRSAAuthentication no</code>	Disables Rhost authentication (not needed for key-based authentication)
<code>#ChallengeResponseAuthentication yes</code>	<code>ChallengeResponseAuthentication no</code>	(not needed for key-based authentication)

Default	Replace with	Modification Notes
#UsePAM yes	UsePAM no	(not needed for key-based authentication)
#StrictModes yes	StrictModes yes	Ensures that files and folders are adequately protected by the server's permissions' scheme
#LoginGraceTime 2m	LoginGraceTime 30	Reduces the time allowed to authenticate to 30 seconds
#KeyRegenerationInterval 1h	KeyRegenerationInterval 3600	Ensures that the server key is changed frequently
#ServerKeyBits 768	ServerKeyBits 768	Requires that the server key is 768 bits long
#Protocol 2,1	Protocol 2	Restricts OpenSSH so that it only uses SSH2
	AllowUsers <i>username</i>	You have to add this line. Replace <i>username</i> with the name of the account you want to log in as.

Note: When replacing the original values, you have to remove the #.

- 10 On the client, enter the following command:

```
$ sudo pico /private/etc/sshd_config
```

Authenticate, if requested.

- 11 On the client, edit the following lines:

Default	Replace with	Modification Notes
#PasswordAuthentication yes	PasswordAuthentication no	Disables password authentication
#RSAAuthentication yes	RSAAuthentication no	Disables RSA authentication (not needed for key-based authentication)

- 12 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.

Note: when you connect to a host using the IP address a entries will be created in the `ssh_known_hosts` file. If you connect to the same host using its host name a separate entry will be created in the `ssh_known_host` file. Each connection is treated as a unique connection.

If successful, you will be prompted to enter your passphrase for the key.

Preventing Connections 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 to which you are allowed to connect, 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:

```
$ rm ~/.ssh/known_hosts
```

- 3 Use SSH to connect to every server you want to allow access to. For each server, enter 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.

Note: when you connect to a host using the IP address, entries will be created in the `ssh_known_hosts` file. If you connect to the same host using its host name, a separate entry will be created in the `ssh_known_hosts` file. Each connection is treated as a unique connection.

You will be 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
```

- 4 Enter the following command:

```
$ sudo cp ~/.ssh/known_hosts /etc/ssh_known_hosts
```

Authenticate, if requested.

Because `ssh_known_hosts` is located in `/etc/`, users can't modify this file unless they have administrator access.

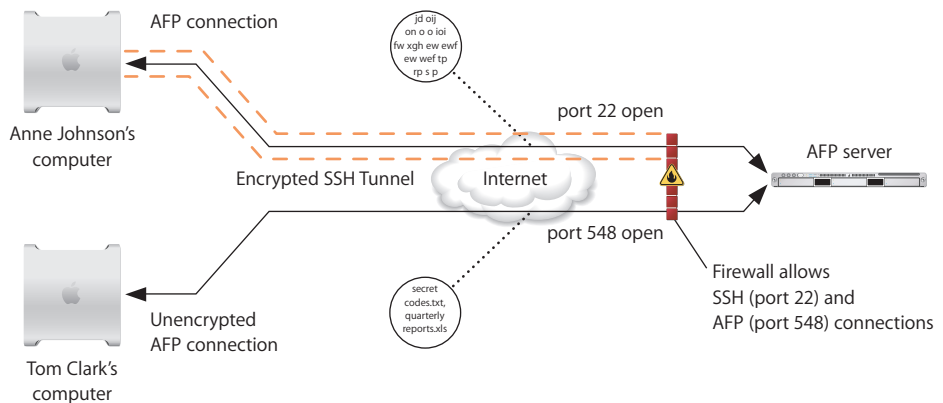
- 5 Enter the following command:

```
$ rm ~/.ssh/known_hosts
```

After you remove `~/.ssh/known_hosts`, your computer will only connect to servers listed in `/etc/ssh_known_hosts`.

Using SSH as a Tunnel

SSH can be used 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 unsecure network (such as the Internet).



For 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. Once 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 and replace *RemoteAFPAccount* with the AFP account name.

Enter the password for *RemoteAFPAccount* when prompted.

- 3 Create a new server in AFP.

Enter the address `localhost:2501` and *RemoteAFPAccount* username and password.

Securing Bonjour

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 also provides information about your available services.

Users and applications on your local network can use Bonjour to quickly determine which services are available on your computer. Although this might seem like a security risk, malicious intruders can use their own tools, such as port scanners, to locate the same services advertised by Bonjour. You should disable any unused services that you don't want others to discover through Bonjour.

To secure Bonjour, you must secure your local network. You should only connect to secure, trusted local networks. You should also check Network preferences to ensure you only enable required networking connections. This helps reduce the chance of accidentally connecting to an insecure network.

Before using Bonjour to connect to a service, you should verify that the service is legitimate, and not spoofed. If you connect to a spoofed service, you might inadvertently download malicious files.

Enter the following command to disable Bonjour:

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

You won't be able to use network printing using Bonjour, so you'll have to manually configure network printers. This can also disable some functionality in other applications that rely on Bonjour, or possibly make them unusable. For example, there are issues with calendar and address book sharing, and finding iChat buddies.

If disabling Bonjour causes vital applications to break, enter the following command to reenable Bonjour:

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

If you decide to re-enable Bonjour, block UDP port 5353 on your firewall to block externally-originating Bonjour traffic.

Securing Network Services

By default, none of the network services listed in Sharing preferences are enabled and their respective ports are closed. Carefully choose which network services you want to enable. As you enable more services, you open more ports and increase the chance of network intrusion. Additionally, each service has specific security issues that you should be aware of. Improperly configured network services are a major security risk.

WARNING: Network services listed in Sharing preferences should only be enabled in a secure environment, and only when the service is absolutely needed.

Securing AFP

When connecting to an AFP share point, you authenticate with the AFP share point by using the strongest available authentication method. Usually, if you are connecting to another Mac OS X computer, your password will be encrypted during transmission. However, some AFP servers might require that you send clear text passwords. You can require that passwords not be sent in clear text.

By default, data is sent over AFP in unencrypted format. If you're connecting to a computer using Mac OS X Server to run an AFP share point, you can use SSH to automatically encrypt data before transferring it. If the computer you are connecting to runs an AFP share point by enabling Personal File Sharing, you cannot use SSH for AFP. Enabling SSH for AFP can negatively impact performance. However, enabling data encryption with SSH secures data sent to and received from AFP share points.

To secure your connection to AFP share points:

- 1 In Finder, choose Go > Connect to Server.
- 2 In the share point selection window, select the AFP share point and click Connect. The AFP share point you select should have SSH enabled.
- 3 In the authentication window, choose Options from the action pop-up menu.
- 4 Deselect "Allow sending password in clear text."
- 5 Select "Allow secure connections using SSH."
- 6 Select "Warn when connection does not support SSH."
- 7 Click OK.
- 8 In the authentication window, enter your name and password. Click Connect.

Securing Windows Sharing

Windows sharing allows users to access shared files and printers by using the SMB/CIFS protocol. You should not enable Windows sharing, because there are well-known risks associated with SMB/CIFS. For example, SMB/CIFS uses NTLMv1 and NTLMv2 encryption, both of which are very weak password hashing schemes.

When you enable Windows sharing, Mac OS X describes the dangers associated with SMB/CIFS.

Securing Personal Web Sharing

Personal Web Sharing allows any user on the network to view files you store in `~/Sites/`. To secure this service, you should be familiar with securing the Apache web server. You should also consider setting up SSL to encrypt web traffic. To set up SSL, you'll need an x.509 certificate.

If you plan to use Personal Web Sharing mainly for file sharing, you should consider using the Remote Login `sftp` command-line tool. The `sftp` command-line tool is much more secure than Personal Web Sharing. For more information, enter `man sftp` in a Terminal window and see “Securing Remote Login” on page 128.

Securing Remote Login

Remote Login allows users to connect to your computer through SSH. By enabling Remote Login, you activate more secure versions of some 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 “Securing SSH” on page 120.

Securing FTP Access

The File Transfer Protocol (FTP) is an insecure tool used for file sharing that should not be enabled. When you authenticate with most FTP servers, your password is sent in clear text format. A computer with Mac OS X Server that provides FTP service can use Kerberos-based authentication. Although Kerberos provides secure authentication, data sent over FTP is still not secure. You should disable FTP service to prevent the chance of sending clear text passwords over a network.

Instead of using FTP, consider using the `sftp` or `scp` command-line tools. These tools securely authenticate, and also securely transfer files. For more information, see “Securing Remote Login” on page 128.

Securing Apple Remote Desktop

Apple Remote Desktop is an easy-to-use, powerful, open standards-based, desktop management tool. It provides several security mechanisms, including AES-128 encryption, that ensure you can use the tool securely and that all data is securely transferred to and from client and administrator computers.

For more information, see the Apple Remote Desktop administration guide.

Securing Remote Apple Events

If you enable Remote Apple Events, you are allowing 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.

You should not enable Remote Apple Events. If you do, you should do so on a trusted private network and disable it immediately after disconnecting from the network.

Securing Printer Sharing

Printer Sharing allows users on other computers to access printers connected to your computer. You should 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.

Securing Xgrid

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, while an agent processes jobs received from an Xgrid controller. A controller is a server that receives jobs from clients, and distributes jobs to agents.

When you volunteer your computer as an agent, or when you run a grid-enabled application as a client, you should always explicitly specify the controller by name or address. Although your computer can use Bonjour to automatically discover controllers on the local network, when you explicitly specify a controller, you help ensure that your computer connects to the intended Xgrid controller, and not a malicious controller. While it is possible for a malicious controller to spoof a legitimate controller's DNS and IP address, choosing a specific controller prevents trivial attacks.

Your computer can specify the type of authentication that it requires, including password, Kerberos, or no authentication. If you are connecting your computer to the Internet, you should require some form of authentication, because choosing no authentication might result in unknowingly connecting to a malicious controller. These 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 any sensitive data they contain) hijacked by malicious agents.

You should 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, all communication with the controller is transmitted in clear text. If your connection uses Kerberos authentication, only the authentication with the controller is encrypted.

For more information about Xgrid, see the Xgrid administration guide.

Intrusion Detection Systems

An intrusion detection system (IDS) monitors user activity and examines data received through the network. You are notified of any 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) and network-based intrusion detection systems (NIDS). 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. A NIDS examines individual network packets, and compares them against a database of known attack patterns.

For more information, see "Intrusion Protection Using Open Source Tools" (www.apple.com/itpro/articles/intrusionprotection/index2.html).

Monitoring events and logs can help to protect the integrity of your computer.

Using auditing and logging tools to monitor your computer can help you secure your computer. By reviewing these audits and log files, you can stop login attempts from unauthorized users or computers, and further lock down your configuration settings. This chapter also discusses antivirus tools, which detect unwanted viruses.

About Activity Analysis Tools

Mac OS X includes several command-line tools that you can use to analyze computer activity.

Depending on the tools' configurations and your computer's activity, running these tools can use a lot 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 thereby circumvent the tool.

If your computer contains sensitive data, you should consider using both auditing and logging tools. By using both types of tools, you'll be able to properly research and analyze intrusion attempts and changes in your computer's behavior. You must configure these tools to meet your organization's needs, and then change their logging settings to create only relevant information for reviewing or archiving purposes.

Using Auditing Tools

Auditing is the capture and maintenance of information about security-related events. Auditing helps determine the causes and the methods used for both successful and failed access attempts.

Mac OS X includes a suite of auditing tools that allow you to manage, refine, and view auditing logs. The auditing tools require an optional installation from the installation disc. For information about these auditing tools, see the *Common Criteria Configuration and Administration Guide*, available at www.apple.com/support/security/commoncriteria/.

Configuring Log Files

Logging is the recording of various events, including changes to service status, processes, and operating system components. Some of these 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, the 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. Some `sudo` commands perform additional actions that are not logged. You should restrict the `sudo` commands that individual users are allowed to use. For more information, see "Securing the System Administrator Account" on page 46.

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 displays a pane that shows other log files on the system in a tree view. The tree includes folders for services such as web and email server software.

Mac OS X log files are handled either by the BSD subsystem or by a specific application. The BSD subsystem handles most of the 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 transferred over the network to a dedicated log server that stores them. Using remote logging is strongly recommended.

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 three types of data: a facility, a priority, and an action.

- Facilities are categories of log messages. The 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: debug, info, notice, warning, err, crit, alert, and emerg. The priority of the log message is set by the application sending it, not `syslogd`.
- The action specifies what to do with a log message of a specific facility and priority. Messages can be sent to files, named pipes, devices, or to a remote host.

The following sample line specifies that for any log messages in the category “mail,” with a priority of “emerg” or higher, the message will be written to the `/var/log/mail.log` file:

```
mail.emerg /var/log/mail.log
```

The facility and priority are separated by only a period, and these are separated from the action by one or more tabs. Wildcards (“*”) can also be used in the configuration file. The following sample line logs all 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/syslog.conf` is configured for local logging in the `/var/log` folder. The computer is set to rotate log files using a cron job at the time intervals specified in the `/etc/crontab` file. Rotation entails compressing the current log file, incrementing the integer in the filename of compressed log files, and creating a new log file for new messages.

The following table describes the rotation process after two rotations.

Files before rotation:	Files after first rotation:	File after second rotation:
system.log	system.log	system.log
mail.log	mail.log	mail.log
	mail.log.1.gz	mail.log.1.gz
	system.log.1.gz	system.log.1.gz
		mail.log.2.gz
		system.log.2.gz

The log files are rotated by a cron job, and the rotation only occurs if the computer is on when the job is scheduled. By default, the log rotation tasks are scheduled for very early in the morning (for example, 4:30 a.m. on Saturday) to be as unobtrusive as possible to the end user. If the system will not be powered on at this time, adjust the settings in `/etc/crontab`.

For information about editing the `/etc/crontab` file, issue the `man 5 crontab` command in a Terminal window. The following line shows the default for running the weekly log rotation script, which is configured for 4:15 a.m. on the last day of the week, Saturday (Sunday is 0). An asterisk denotes “any,” so a line of all asterisks would execute every minute.

```

                DayOf      DayOf
#Minute Hour Month Month Week User Command
    15 4 * * 6 root periodic weekly
```

The following line would change the time to 12:15 p.m. on Tuesday, when the computer is much more likely to be on:

```

                DayOf      DayOf
#Minute Hour Month Month Week User Command
          15 12 * * 2 root periodic weekly
```

Remote System Logging

You should use remote logging in addition to local logging for any computer because local logs can easily be altered if the computer is compromised.

Several security issues must also be considered when making the decision to 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 has been established, and if they are regularly monitored for such activity.

If these security issues outweigh the security benefit of remote logging for the network being configured, then remote logging should not be used.

The following instructions assume a remote log server has been configured 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 actual name or IP address of the log server. Make sure to keep 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
```

About File Integrity Checking Tools

File integrity tools help protect your computer by detecting and logging all 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 any kernel modules. Depending on the file integrity tool you choose, you can also use advanced features, such as the ability to reverse individual file system changes, or to receive highly detailed logs in a variety of formats.

File integrity tools are generally hosted on a server that you securely connect your computer to. The server retrieves logs from all clients, and stores baseline configuration databases and current configuration data.

For more information about checksum and file hashing, see “Verifying the Integrity of Software” on page 28

About Antivirus Tools

Installing antivirus tools helps prevent infection of your computer by viruses, and help prevent your computer from becoming a host for spreading viruses to other computers. These tools quickly identify suspicious content and compare them against known malicious content.

In addition to using antivirus tools, you should develop computer usage habits that are not prone to virus infection. For example, don't download or open content you didn't specifically request, and never open a file sent to you by someone you don't know. For more information about securely using email, see “Email, Chat, and Other Online Communication Guidelines” on page 152.

When you use antivirus tools, make sure you have the latest virus definition files. The protection provided by your antivirus tool depends on the quality of your virus definition files. If your antivirus program supports it, enable automatic downloading of virus definitions.

For a list of antivirus tools, see the *Macintosh Products Guide* at guide.apple.com.

This appendix contains a checklist of recommended steps required to secure Mac OS X.

This appendix contains checklists of all the 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, you can use the “Notes” column to justify or clarify your deviation.

Installation Action Items

For details, see Chapter 2, “Installing Mac OS X,” on page 21.

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 any unnecessary packages		
Do not transfer confidential information in Setup Assistant		
Do not connect to the Internet		
Create administrator accounts with difficult-to-guess names		
Create complex passwords for administrator accounts		
Do not enter a password-related hint; instead, enter help desk contact information		
Enter correct time settings		

Action Item	Completed?	Notes
Use an internal Software Update server		
Update system software using verified packages		
Repair disk permissions after installing software or software updates		

Hardware and Core Mac OS X Action Items

For details, see Chapter 3, “Protecting Hardware and Securing Global System Settings,” on page 31.

Action Item	Completed?	Notes
Restrict access to rooms that have computers		
Store computers in locked or secure containers when not in use		
Remove Mac OS 9		
When needed, run Mac OS 9 from a CD or a disc image		
Require an Open Firmware or EFI password		
Create an access warning for the login window		
Create an access warning for the command line		

Account Configuration Action Items

For details, see Chapter 4, “Securing Accounts,” on page 41.

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 appropriate parental controls for managed accounts		

Action Item	Completed?	Notes
Restrict <code>sudo</code> users to being able to access only required commands		
Securely configure LDAPv3 access		
Securely configure Active Directory access		
Use Password Assistant to help generate complex passwords		
Authenticate using a smart card, token, or biometric device		
Set a strong password policy		
Secure the login keychain		
Secure individual keychain items		
Create specialized keychains for different purposes		
Use a portable drive to store keychains		

Securing System Software Action Items

Chapter 5, “Securing System Preferences,” describes how to secure system preferences. Every system preference with security-related configuration settings has its own action item checklist.

.Mac Preferences Action Items

For details, see “Securing .Mac Preferences” on page 61.

Action Item	Completed?	Notes
Disable all Sync options		
Disable iDisk Syncing		
Enable Public Folder password protection		
Do not register computers for synchronization		

Accounts Preferences Action Items

For details, see “Securing Accounts Preferences” on page 63.

Action Item	Completed?	Notes
Change initial password for the system administrator account		
Disable automatic login		
Display login window as name and password		
Disable “Show the Restart, Sleep, and Shut Down buttons”		
Disable “Show password hints”		
Disable “Enable fast user switching”		

Appearance Preferences Action Items

For details, see “Securing Appearance Preferences” on page 66.

Action Item	Completed?	Notes
Do not display recent applications		
Do not display recent documents		
Do not display recent servers		

Bluetooth Preferences Action Items

For details, see “Securing Bluetooth Preferences” on page 67.

Action Item	Completed?	Notes
Disable Bluetooth by using System Preferences for each user account		
Remove privileges to modify Bluetooth preferences		

CDs & DVDs Preferences Actions Items

For details, see “Securing CDs & DVDs Preferences” on page 68.

Action Item	Completed?	Notes
Disable automatic actions for blank CDs for each user account		
Disable automatic actions for blank DVDs for each user account		
Disable automatic actions for music CDs for each user account		
Disable automatic actions for picture CDs for each user account		
Disable automatic actions for video DVDs for each user account		
Remove privileges to modify CDs & DVDs preferences		

Classic Preferences Action Items

For details, see “Securing Classic Preferences” on page 69.

Action Item	Completed?	Notes
Disable starting Classic at login		
Do not hide Classic when starting		
Warn before starting Classic		
Show Classic status in the menu bar		
Turn off Classic extensions		
Use the Memory/Versions pane to view all applications running in Mac OS 9		

Dashboard and Exposé Preferences Action Items

For details, see “Securing Dashboard and Exposé Preferences” on page 71

Action Item	Completed?	Notes
Do not set any screen corner to Disable Screen Saver for each user account		
Set a screen corner to Start Screen Saver for each user account		
Remove privileges to modify Dashboard & Exposé System Preferences		

Date & Time Preferences Action Items

For details, see “Securing Date & Time Preferences” on page 72.

Action Item	Completed?	Notes
Set the correct date and time		
Use a secure internal NTP server for automatic date and time setting		

Desktop & Screen Saver Preferences Action Items

For details, see “Securing Desktop & Screen Saver Preferences” on page 74.

Action Item	Completed?	Notes
Set a short inactivity interval for the screen saver		
Do not set any screen corner to Disable Screen Saver for each user account		
Set a screen corner to Start Screen Saver for each user account		
Remove privileges to modify Dashboard & Exposé preferences		

Dock Preferences Action Items

For details, see “Securing Dock Preferences” on page 76.

Action Item	Completed?	Notes
Enable “Automatically hide and show the Dock”		

Energy Saver Preferences Action Items

For details, see “Securing Energy Saver Preferences” on page 77.

Action Item	Completed?	Notes
Disable sleeping the computer for all power settings		
Enable sleeping the display for all power settings		
Enable sleeping the hard disk for all power settings		
Disable “Wake when the modem detects a ring” for all power settings		
Disable “Wake for Ethernet network administrator access” for power adapter settings		
Disable “Restart automatically after a power failure” for all power settings		

Securing International Preferences

For details, see “Securing International Preferences” on page 78.

Action Item	Completed?	Notes
Check the security risk of the language character set		

Securing Keyboard & Mouse Preferences

For details, see “Securing Keyboard & Mouse Preferences” on page 79.

Action Item	Completed?	Notes
Disable “Allow Bluetooth devices to wake this computer”		

Network Preferences Action Items

For details, see “Securing Network Preferences” on page 80.

Action Item	Completed?	Notes
Disable AirPort		
Disable Bluetooth		
Disable IPv6		

Print & Fax Preferences Action Items

For details, see “Securing Print & Fax Preferences” on page 82.

Action Item	Completed?	Notes
Only use printers in secure locations		
Disable receiving faxes		
Disable printer sharing		
Disable sending faxes		

QuickTime Preferences Action Items

For details, see “Securing QuickTime Preferences” on page 84.

Action Item	Completed?	Notes
Disable “Save movies in disk cache”		
Do not install third-party QuickTime software		

Security Preferences Action Items

For details, see “Securing Security Preferences” on page 85.

Action Item	Completed?	Notes
Enable FileVault for every account		
Require a password to wake the computer from sleep or screen saver for each account		
Disable automatic login		
Require a password to unlock each secure system preference		
Disable automatic logout after a period of inactivity		
Use secure virtual memory		
Disable remote control infrared receiver		
Securely erase old swap files		

Sharing Preferences Action Items

For details, see “Securing Sharing Preferences” on page 87.

Action Item	Completed?	Notes
Change the computer name		
Enable firewall protection for services used		
Disable Internet Sharing		

Software Update Preferences Action Items

For details, see “Securing Software Update Preferences” on page 90.

Action Item	Completed?	Notes
Disable “Check for updates”		
Disable “Download important updates in the background”		
Use an internal Software Update server		
Transfer installer packages from a test-bed computer		
Verify installer packages before installing		

Sound Preferences Action Items

For details, see “Securing Sound Preferences” on page 91.

Action Item	Completed?	Notes
Change sound input device to Line In		
Minimize input volume for the internal microphone		
Minimize input volume for the audio line-in port		

Speech Preferences Action Items

For details, see “Securing Speech Preferences” on page 92.

Action Item	Completed?	Notes
Only enable speech recognition in a secure environment		
Use headphones if you enable text to speech		

Spotlight Preferences Action Items

For details, see “Securing Spotlight Preferences” on page 93.

Action Item	Completed?	Notes
Prevent Spotlight from searching all confidential folders		

Startup Disk Preferences Action Items

For details, see “Securing Startup Disk Preferences” on page 95.

Action Item	Completed?	Notes
Carefully choose the startup volume		

Data Maintenance and Encryption Action Items

For details, see Chapter 6, “Securing Data and Using Encryption,” on page 97.

Action Item	Completed?	Notes
Mandate setting POSIX permissions for files		
Mandate setting ACL permissions for files		
Change the global umask value		
Enable FileVault for every user		
Encrypt portable files		
Mandate secure erasing of files		
Mandate secure erasing of partitions		
Mandate secure erasing of free space		

Network Services Configuration Action Items

For details, see Chapter 7, “Securing Network Services,” on page 113.

Action Item	Completed?	Notes
Configure Mail to only send signed and encrypted email		
Configure Mail to disable the display of remote images		

Action Item	Completed?	Notes
Configure Safari to disable AutoFill, not use cookies, and ask before sending nonsecure forms		
Always use Safari's Private Browsing and frequently empty Safari's cache		
Update iChat by upgrading to Mac OS X version 10.4.3 or later, and use .Mac accounts with a Secure iChat certificate		
Configure VPN to use L2TP over IPSec		
Configure the firewall to block both TCP and UDP communication, log firewall activity, and enable Stealth mode		
Disable Internet Sharing		
Enable TCP wrappers per service		
Configure SSH to only allow key-based authentication		
Configure AFP so that it does not allow sending passwords in clear text, and allows secure connections using SSH		
Disable Windows Sharing		
Disable Personal Web Sharing		
Use secure Remote Login tools instead of their insecure equivalents		
Disable FTP access		
Securely configure Apple Remote Desktop		
Disable Remote Apple Events		
Disable Printer Sharing		
Configure Xgrid to use Kerberos authentication		
Use a host-based intrusion detection system		
Use a network-based intrusion detection system		

System Integrity Validation Action Items

For details, see Chapter 8, “Validating System Integrity,” on page 131.

Action Item	Completed?	Notes
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		

This appendix contains best practices for passwords and computer usage.

Passwords are a common method of authenticating with another computer. This appendix explains how to create, store, and manage passwords. It also discusses communication and computer usage guidelines.

Password Guidelines

Many applications and services require that you create passwords to authenticate. Mac OS X includes applications that help create complex passwords (Password Assistant), and securely store your passwords (Keychain Access).

Creating Complex Passwords

Use the following tips to create complex passwords:

- Use a mixture of alphabetic (upper and lower case), numeric, and special characters (such as ! and @).
- Don't use words or combinations of words found in a dictionary of any language. Also, don't use names or anything else that is intelligible.
- Create a password of at least twelve characters. Long passwords are generally more secure than shorter passwords.
- Create as random a password as possible.

You can use Password Assistant to verify the complexity of your password. For more information, see "Using Password Assistant" on page 51.

Using an Algorithm to Create a Complex Password

Consider creating an algorithm to make a complex (but memorable) password. Using an algorithm can increase the randomness of your password. Additionally, instead of having to remember a complex password, you must remember only the algorithm.

The following example shows one possible algorithm for creating a complex password. Instead of using this algorithm, create your own or modify this one.

The following is an algorithm for creating a complex password:

- 1 Choose your favorite phrase or saying.

In this example, we'll use:

Four score and seven years ago our fathers brought forth

Ideally you should choose a phrase of at least eight words.

- 2 Reduce your favorite phrase to an acronym by keeping only the first letter of each word.

The sample phrase becomes:

Fsasyaofbf

- 3 Replace a letter with a number.

If we replace "F" (from "Four") with "4," the last "f" (from "forth") with "4th," and "s" (from "seven") with "7," the sample phrase becomes:

4sa7yaofb4th

- 4 Add special characters or numbers that resemble a letter.

If we replace "s" (from "score") with "\$" and "a" (from "and") with "&" the sample phrase becomes:

4\$&7yaofb4th

- 5 Add special characters or numbers that sound or look like a letter.

If we replace "a" (from "ago") with "@" and "o" (from "our") with "0" the sample phrase becomes:

4\$&7y@0fb4th

- 6 Make some letters uppercase.

If we convert all vowels to uppercase, the sample phrase becomes:

4\$&7Y@0Fb4Th

Safely Storing Your Password

If you store your password or the algorithm used to make your password in a safe place, you'll be able to create more complex passwords without the fear of being unable to recover forgotten passwords. When storing passwords, make sure your storage location is safe, unknown, and inaccessible to intruders. Consider storing your passwords in a sealed envelope within a locked container.

Don't store your password anywhere near your computer.

When writing down your password, take the following precautions:

- Don't identify the password as being a password.
- Don't include account information on the same piece of paper.
- Add some false characters or misinformation to the written password in a way that you remember. Make the written password different from the real password.
- Never record a password online, and never send a password to another person through email.

You can use Keychain Access to store your more complex, longer passwords. You'll still need a password to unlock Keychain Access so that you can view and use these passwords. Because Keychain Access requires that you authenticate to unlock keychains, it is both convenient for you and inaccessible to intruders. Store the Keychain Access password in a safe location. For more information, see "Storing Credentials" on page 53.

Password Maintenance

After you create a good password and store it in a safe location, do the following to make sure your password remains secure:

- Never tell anyone your password. If you tell someone your password, immediately change your password.
- Change your password frequently, and whenever you think your password might be compromised. If your account is compromised, notify authorities and close the account.
- Be aware of when trusted applications ask for your password. Malicious applications can mimic a trusted application and ask you for your password when you're not expecting it.
- Don't reuse the same password for multiple accounts. Otherwise an intruder who compromises your password can use the password for all of those accounts.
- Don't enter password-related hints in "password hint" fields. By providing a hint, you compromise the integrity of your password.
- Don't access your account on public computers or other computers that you don't trust. Malicious computers can record your keystrokes.
- Don't enter your password in front of other people.

Email, Chat, and Other Online Communication Guidelines

Be especially careful when sending and receiving email, instant messages, or any other kind of online communication. Online communication devices can be exploited by intruders who send you malicious files that compromise your computer's integrity. They can also phish for information, which can be used to compromise account integrity and confidential information.

When you communicate online:

- Don't download or open content you didn't specifically request, and never open a file sent to you by someone you don't know. For more information about safely receiving email attachments, see AppleCare Knowledge Base article #108009, "Safety tips for handling email attachments and content downloaded from the Internet" (www.apple.com/support/).
- Be aware of the level of security provided by your chosen communication medium. You should at least know if you are communicating securely or insecurely.
- Don't send confidential information over insecure channels like unencrypted email and web forms, or through insecure network connections.
- Don't use your personal email or chat services to send or receive confidential business information.
- Don't communicate anything that can be used to compromise your identity or your password. You should only discuss personal or confidential information with verified individuals who have a specific need to know the information.

Computer Usage Guidelines

You can improve security through more secure work habits. For example:

- Follow all security guidelines set by your organization.
- Only install applications, other software, and hardware that are allowed by your organization. After installing applications, repair disk permissions. For more information, see "Using Disk Utility to Repair Disk Permissions" on page 30.
- If Safari, Mail, or iChat warns you about downloading an application, verify the authenticity of the application before you open it. Contact your organization's IT staff if the file is suspicious.
- Don't reconfigure settings unless you need to. Check with your organization to see if your desired settings will have any security ramifications.
- Work with confidential data behind closed doors. If an unauthorized person can see your display, turn off your display, use Exposé to display your desktop, or open Finder and choose Finder > Hide Others. If you must work with other people nearby, try using a security lens or screen overlay.

- Separate your confidential and personal usage between accounts. You should have an account dedicated to performing secure tasks, like confidential work, and you should have another account that you use to do less secure tasks, like personal errands.
- Disable your computer when you're away from it. Either turn off the computer, or enable a password-protected screensaver. For more information, see "Securing Desktop & Screen Saver Preferences" on page 74.
- Log out of secure accounts when you aren't using them, or when you leave your computer.
- Be aware of the latest security news from Apple. Consider joining the Security Announce mailing list at lists.apple.com/mailman/listinfo/security-announce. To join this list, you'll need to use the Apple Product Security PGP key. For information, see "How to use the Apple Product Security PGP Key" for docs.info.apple.com/article.html?artnum=25314.

This glossary defines terms and spells out abbreviations you may encounter while working with online help or the various reference manuals for Mac OS X Server. References to terms defined elsewhere in the glossary appear in italics.

access control A method of controlling which computers can access a network or network services.

ACE Access Control Entry. An entry within the ACL that controls access rights. See **ACL**.

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

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined “admin” group.

administrator computer A Mac OS X computer onto which you’ve installed the server administration applications from the Mac OS X Server Admin CD.

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

authentication The process of proving a user’s identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user’s level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

authentication authority attribute A value that identifies the password validation scheme specified for a user and provides additional information as required.

authorization The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an authentication process proves the user’s identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

BIND Berkeley Internet Name Domain. The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

binding (n.) A connection between a computer and a directory domain for the purpose of getting identification, authorization, and other administrative data. (v.) The process of making such a connection. See also **trusted binding**.

biometrics A technology that authenticates a person's identity based on unique physiological or behavioral characteristics. Provides an additional factor to authentication. See **two-factor authentication**.

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

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

buffer caching Holding data in memory so that it can be accessed more quickly than if it were repeatedly read from disk.

cache A portion of memory or an area on a hard disk that stores frequently accessed data in order to speed up processing times. Read cache holds data in case it's requested by a client; write cache holds data written by a client until it can be stored on disk. See also **buffer caching**, **controller cache**, **disk cache**.

certificate Sometimes called an "identity certificate" or "public key certificate." A file in a specific format (Mac OS X Server uses the x.509 format) that contains the public key half of a public-private keypair, the user's identity information such as name and contact information, and the digital signature or either a *Certificate Authority* (CA) or the key user.

Certificate Authority An authority that issues and manages digital certificates in order to ensure secure transmission of data on a public network. See also **public key infrastructure and certificate**.

cluster A collection of computers interconnected in order to improve reliability, availability, and performance. Clustered computers often run special software to coordinate the computers' activities. See also **computational cluster**.

computational cluster A group of computers or servers that are grouped together to share the processing of a task at a high level of performance. A computational cluster can perform larger tasks than a single computer would be able to complete, and such a grouping of computers (or "nodes") can achieve high performance comparable to a supercomputer.

controller In an Xsan storage area network, short for metadata controller. In RAID systems, controller refers to hardware that manages the reading and writing of data. By segmenting and writing or reading data on multiple drives simultaneously, the RAID controller achieves fast and highly efficient storage and access. See also **metadata controller**.

controller cache A cache that resides within a controller and whose primary purpose is to improve disk performance.

cracker A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to hacker.

crypt password A type of password that's stored as a hash (using the standard UNIX encryption algorithm) directly in a user record.

daemon A program that runs in the background and provides important system services, such as processing incoming email or handling requests from the network.

decryption The process of retrieving encrypted data using some sort of special knowledge. See also **encryption**.

deploy To place configured computer systems into a specific environment or make them available for use in that environment.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a lease period—the length of time the client computer may use the address.

directory Also known as a folder. A hierarchically organized list of files and/or other directories.

disk cache A cache that resides within a disk. See also **cache**, **controller cache**.

disk image A file that, when opened, creates an icon on a Mac OS X desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

DoS attack Denial of service attack. An Internet attack that uses thousands of network pings to prevent the legitimate use of a server.

drop box A shared folder with privileges that allow other users to write to, but not read, the folder's contents. Only the owner has full access. Drop boxes should be created only using AFP. When a folder is shared using AFP, the ownership of an item written to the folder is automatically transferred to the owner of the folder, thus giving the owner of a drop box full access to and control over items put into it.

Dynamic Host Configuration Protocol See **DHCP**.

encryption The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications. See also **decryption**.

EFI Extensible Firmware Interface. Software that runs automatically when an Intel-based Macintosh first starts up. It determines the computer's hardware configuration and starts the system software.

Ethernet A common local area networking technology in which data is transmitted in units called packets using protocols such as TCP/IP.

file server A computer that serves files to clients. A file server may be a general-purpose computer that's capable of hosting additional applications or a computer capable only of serving files.

firewall Software that protects the network applications running on your server. IP firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

firmware Software that's stored in read-only memory (ROM) on a device and helps in starting up and operating the device. Firmware allows for certain changes to be made to a device without changing the actual hardware of the device.

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

hacker An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

hash (noun) A scrambled, or encrypted, form of a password or other text.

host Another name for a server.

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

HTTP Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. The HTTP protocol provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

ICMP Internet Control Message Protocol. A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

image See **disk image**.

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

installer package A file package with the filename extension .pkg. An installer package contains resources for installing an application, including the file archive, Read Me and licensing documents, and installer scripts.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

IPv4 See **IP**.

IPv6 Internet Protocol version 6. The next-generation communication protocol to replace IP (also known as IPv4). IPv6 allows a greater number of network addresses and can reduce routing loads across the Internet.

JBoss A full-featured Java application server that provides support for Java 2 Platform, Enterprise Edition (J2EE) applications.

KDC Kerberos Key Distribution Center. A trusted server that issues Kerberos tickets.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

kernel The part of an operating system that handles memory management, resource allocation, and other low-level services essential to the system.

key frame A sample in a sequence of temporally compressed samples that doesn't rely on other samples in the sequence for any of its information. Key frames are placed into temporally compressed sequences at a frequency that's determined by the key frame rate.

L2TP Layer Two Tunneling Protocol. A network transport protocol used for VPN connections. It's essentially a combination of Cisco's L2F and PPTP. L2TP itself isn't an encryption protocol, so it uses IPSec for packet encryption.

LAN Local area network. A network maintained within a facility, as opposed to a WAN (wide area network) that links geographically separated facilities.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

managed network The items managed clients are allowed to "see" when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a "network view."

metadata controller The computer that manages metadata in an Xsan storage area network.

mutual authentication Also known as two-way authentication. A type of authentication in which two parties authenticate with each other. For example, a client or user verifies their identity to a server, and that server confirms its identity to the client or user. Each side has the other's authenticated identity.

NAT Network Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications.

NetBoot server A Mac OS X server on which you've installed NetBoot software and have configured to allow clients to start up from disk images on the server.

Network File System See **NFS**.

network view See **managed network**.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

node A processing location. A node can be a computer or some other device, such as a printer. Each node has a unique network address. In Xsan, a node is any computer connected to a storage area network.

NTP Network time protocol. A network protocol used to synchronize the clocks of computers across a network to some time reference clock. NTP is used to ensure that all the computers on a network are reporting the same time.

object class A set of rules that define similar objects in a directory domain by specifying attributes that each object must have and other attributes that each object may have.

offline Refers to data that isn't immediately available, or to devices that are physically connected but not available for use.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, NetInfo, or Active Directory protocols; BSD configuration files; and network services.

Open Directory master A server that provides LDAP directory service, Kerberos authentication service, and Open Directory Password Server.

Open Directory Password Server An authentication service that validates passwords using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

partition A subdivision of the capacity of a physical or logical disk. Partitions are made up of contiguous blocks on the disk.

PDC Primary domain controller. In Windows networking, a domain controller that has been designated as the primary authentication server for its domain.

permissions Settings that define the kind of access users have to shared items in a file system. You can assign four types of permissions to a share point, folder, or file: read/write, read-only, write-only, and none (no access). See also **privileges**.

phishing An attempt to masquerade as a trusted organization or individual to trick others into divulging confidential information.

PKI Public Key Infrastructure. A mechanism that allows two parties to a data transaction to authenticate each other and use encryption keys and other information in identity certificates to encrypt and decrypt messages they exchange.

POP Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

portable home directory A portable home directory provides a user with both a local and network home folder. The contents of these two home folders, as well as the user's directory and authentication information, can be automatically kept in sync.

POSIX Portable Operating System Interface for UNIX. A family of open system standards based on UNIX, which allows applications to be written to a single target environment in which they can run unchanged on a variety of systems.

print queue An orderly waiting area where print jobs wait until a printer is available. The print service in Mac OS X Server uses print queues on the server to facilitate management.

private key One of two asymmetric keys used in a PKI security system. The private key is not distributed and usually encrypted with a passphrase by the owner. It can digitally sign a message or certificate, claiming authenticity. It can decrypt messages encrypted with the corresponding public key. Finally, it can encrypt messages that can only be decrypted by the private key.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

protocol A set of rules that determines how data is sent back and forth between two applications.

proxy server A server that sits between a client application, such as a web browser, and a real server. The proxy server intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

public key One of two asymmetric keys used in a PKI security system. The public key is distributed to other communicating parties. It can encrypt messages that can be decrypted only by the holder of the corresponding private key, and it can verify the signature on a message originating from a corresponding private key.

public key certificate See **certificate**.

public key infrastructure A secure method of exchanging data over an unsecure public network, such as the Internet, by using public key cryptography.

QTSS QuickTime Streaming Server. A technology that lets you deliver media over the Internet in real time.

record type A specific category of records, such as users, computers, and mounts. For each record type, a directory domain may contain any number of records.

recursion The process of fully resolving domain names into IP addresses. A nonrecursive DNS query allows referrals to other DNS servers to resolve the address. In general, user applications depend on the DNS server to perform this function, but other DNS servers do not have to perform a recursive query.

rogue computer A computer that is set up by an attacker for the purpose of infiltrating network traffic in an effort to gain unauthorized access to your network environment.

root An account on a system that has no protections or restrictions. System administrators use this account to make changes to the system's configuration.

router A computer networking device that forwards data packets toward their destinations. A router is a special form of gateway which links related network segments. In the small office or home, the term router often means an Internet gateway, often with Network Address Translation (NAT) functions. Although generally correct, the term router more properly refers to a network device with dedicated routing hardware.

RSA Rivest Shamir Adleman algorithm. A public key encryption method that can be used both for encrypting messages and making digital signatures.

SACL Service Access Control List. Lets you specify which users and groups have access to specific services. See **ACL**.

schema The collection of attributes and record types or classes that provide a blueprint for the information in a directory domain.

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

shadow password A password that's stored in a secure file on the server and can be authenticated using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

shared secret A value defined at each node of an L2TP VPN connection that serves as the encryption key seed to negotiate authentication and data transport connections.

single sign-on An authentication strategy that relieves users from entering a name and password separately for every network service. Mac OS X Server uses Kerberos to enable single sign-on.

smart card A portable security device that contains a microprocessor. The smart card's microprocessor and its reader use a mutual identification protocol to identify each other before releasing information. The smart card is capable of securely storing passwords, certificates, and keys.

SMB/CIFS Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB/CIFS to provide access to servers, printers, and other network resources.

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

SNMP Simple Network Management Protocol. A set of standard protocols used to manage and monitor multiplatform computer network devices.

Spotlight A comprehensive search engine that searches across your documents, images, movies, PDF, email, calendar events, and system preferences. It can find something by its text content, filename, or information associated with it.

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

standalone server A server that provides services on a network but doesn't get directory services from another server or provide directory services to other computers.

static IP address An IP address that's assigned to a computer or device once and is never changed.

streaming Delivery of video or audio data over a network in real time, as a stream of packets instead of a single file download.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration. See also **IP subnet**.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

ticket, Kerberos A temporary credential that proves a Kerberos client's identity to a service.

trusted binding A mutually authenticated connection between a computer and a directory domain. The computer provides credentials to prove its identity, and the directory domain provides credentials to prove its authenticity.

tunneling A technology that allows one network protocol to send its data using the format of another protocol.

two-factor authentication A process that authenticates through a combination of two independent factors: something you know (such as a password), something you have (such as a smart card), or something you are (such as a biometric factor). This is more secure than authentication that uses only one factor, typically a password.

UDP User Datagram Protocol. A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

VPN Virtual Private Network. A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

WAN Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

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

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

zone transfer The method by which zone data is replicated among authoritative DNS servers. Slave DNS servers request zone transfers from their master servers to acquire their data.

.Mac preferences 61–62, 115, 139

A

access control entries. *See* ACEs

access warnings 39–40

See also permissions

accounts

administrator 23–25, 41–42, 45–47

authentication setup 50–59

checklists 138–139, 140

creating secure 43–47

credential storage 53–58

directory domains 47–50

initial setup 24–25

mobile 48

nonadministrator user 41–42

password policies 53

preferences 63–65

types 41

ACEs (access control entries) 29, 101

ACLs (access control lists) 29, 54, 97, 101–102

Active Directory 50

activity analysis tools 131–134

Address Book 49

administrator account 23–25, 41–42, 45–47

Advanced Encryption Standard (AES-128) 85

AFP (Apple Filing Protocol) share points 127

antivirus tools. *See* virus screening

appearance preferences 66, 140

Apple, remote events 87

Apple Remote Desktop (ARD) 87, 129

Apple Software Restore. *See* ASR

applications, securing 44, 113–115

ASR (Apple Software Restore) 23

assistive devices 96

auditing tools 131

authentication 19

accurate time settings 25

Active Directory 50

Directory Access 48–49

overview 19

See also keychains; passwords

server- vs. client-side 114

strengthening methods 50–52

system preferences 60

VPN 116

authorization 18, 19

See also authentication

AutoFill options, disabling 114

automatic actions, disabling 68

B

Berkeley Software Distribution. *See* BSD

Bill of Materials file 30

biometrics-based authentication 52

Bluetooth preferences 67, 140

Bonjour browsing service 126

`boot` command 37

browser security 114–115

BSD (Berkeley Software Distribution) 16

C

cache, browser 114

CDs, preferences 68, 141

CDSA (Common Data Security Architecture) 16

CERT (Computer Emergency Response Team) 15

certificates 18, 105, 113–114, 115

chat service. *See* iChat service

CIFS (Common Internet File System). *See* SMB/CIFS

Classic preferences 69–71, 141

client-side authentication 114

command-line interface

access warnings 40

erasing files 109–110

firewall tool 118

global password policies 53

Mac OS 9 removal 33

ssh access 120–125

startup security setup 38

TCP wrappers 119

command mode startup 37

Common Data Security Architecture. *See* CDSA

Common Security Service Manager. *See* CSSM

Computer Emergency Response Team. *See* CERT

computers

host name 88

- usage guidelines 152
- Console tool 132
- contacts search policy 49
- cookies, disabling 114
- credential storage 53–58
- CSSM (Common Security Service Manager) 18

D

- Dashboard preferences 71–72, 142
- data security 97–110, 146
- Date & Time preferences 72–73, 142
- Desktop preferences 74–75, 142
- digital signature 113–114
- directories. *See* directory services; domains, directory; folders
- Directory Access 48–49
- directory services
 - Active Directory 50
 - directory domains 47–50
 - Open Directory 49
- discovery, service 48
- disk images
 - encrypting 106–107
 - read/write 106
 - restoring from 23
 - running Mac OS 9 from 34
- disks
 - permissions for 28–30
 - startup 95–96, 146
- Disk Utility 30, 109, 111
- display mirroring 76
- Displays preferences 76
- Dock preferences 76, 142
- domains, directory 47–50
- DVDs, preferences 68, 141

E

- EFI (Extensible Firmware Interface) 35, 96
- email. *See* mail service
- encryption 104–108, 113–114, 146
- Energy Saver preferences 77–78, 143
- erasing data permanently 22, 108–110
- Everyone permission level 98
- Exposé preferences 71–72, 142
- Extensible Firmware Interface. *See* EFI

F

- fax preferences 82–83, 144
- files
 - Bill of Materials 30
 - encryption 104–108
 - erasing 108–110
 - integrity checking tools 135
 - managing log 132
 - package 30

- permissions 97–100, 102–103
- file services
 - AFP 127
 - FTP 129
 - See also* FTP; share points
 - SMB/CIFS 87
- file sharing 87
- file systems, erasing data 108
- File Transfer Protocol. *See* FTP
- FileVault 31, 85, 104–105, 121
- FileVault master keychain 105
- fingerprints, server 120, 121
- firewall service 89, 117–118
- FireWire 95
- FireWire Bridge Chip GUID 95
- firmware, open password 21–22, 36–38, 95–96
- flags for files and folders 100–101
- folders
 - flags for 100–101
 - home 47, 104–105
- free disk space, erasing 111
- FTP (File Transfer Protocol) service 87, 129
- full mode startup 37

G

- global file permissions 102–103
- global password policies 53
- grids, server 129–130
- groups, permissions 29, 98
- guest accounts, permissions 98

H

- hard drive 31
- hardware, protection of 31, 138
- HIDS (host-based intrusion detection systems) 130
- HISEC (Highly Secure) templates 50
- home folders 48, 104–105
- host name 88
- hosts. *See* servers
- HTML (Hypertext Markup Language) email 114

I

- iChat service 115
- images. *See* disk images
- installation 21–35, 90, 137–138
- installer packages 90
- instant messaging. *See* iChat service
- Intel-based Macintosh 21, 35
- internal Software Update 25
- International
 - preferences 143
- International preferences 78
- Internet-based Software Update 26
- Internet security
 - .Mac preferences 61–62, 139

- browsers 114–115
- email 113–114, 152–153
- FTP access 129
- instant messaging 115, 152–153
- sharing 87–90, 118, 127–130
- TCP wrappers 119
- VPN 115–117
- intrusion detection system (IDS) monitors 130
- IP addresses 80
- `ipfw` command 118
- IPv6 addressing 80

K

- Kerberos 50, 113
- key-based SSH connection 121–123
- Keyboard & Mouse
 - preferences 143
- Keyboard & Mouse preferences 79
- Keychain Access 53
- keychain services 18, 53–58, 105
- key services 18

L

- L2TP over IPSec protocol 116
- layered security architecture 17
- LDAP (Lightweight Directory Access Protocol) service 49
- LDAPv3 access
- Lightweight Directory Access Protocol. *See* LDAP
- local system logging 133
- locking folders 100
- login
 - access warnings 39–40
 - automatic 85
 - keychain 54–55
 - passwords 53
 - remote 87, 120, 128
 - security measures 63–65, 130
- logs, security 132–134

M

- Mach 16
- Mac OS 9 33–35, 69–71
- mail service 113–114, 152–153
- managed preferences
 - .Mac 61–62, 139
 - Classic 69–71, 141
 - Dashboard 71–72, 142
 - Date & Time 72–73, 142
 - Desktop 74–75, 142
 - Displays 76
 - Dock 76, 142
 - Energy Saver 77–78, 143
 - Exposé 71–72, 142
 - International 78

- Keyboard & Mouse 79
- Network 80–81, 143
- Print & Fax 82–83, 144
- Security 85–86, 144
- Sharing 87–90, 117, 118, 120, 127–130, 145
- Software Update 90
- Software Update service 145
- Sound 91, 145
- Spotlight 93–94, 146
- Startup Disk 95–96, 146
- Universal Access 96
- managed user accounts 41
- Microsoft Windows compatibilities 101
- mobile accounts 48

N

- NetBoot service 23
- network-based directory domains 47–50
- network-based intrusion detection systems. *See* NIDS
- network-based keychains 57–58
- network install image 95
- network services
 - disconnecting for installation 24
 - FileVault limitations 104, 105
 - installation 23
 - keychains 57
 - logs 133–134
 - managed users 43
 - preferences 80–81, 143
 - security methods 113–130, 146–147, 152–153
 - sharing 87–90, 118, 127–130
 - sleep mode security 77
 - Software Update cautions 26
 - wireless preferences 67
- NIDS (network-based intrusion detection systems) 130
- nonadministrator user accounts 41–42
- NTP (network time protocol) 25
- `nvr` tool 38

O

- online communications guidelines 152–153
- Open Directory 49
- Open Firmware interface 36
- Open Firmware password 21–22, 36–38, 95–96
- open source software 16–17
- owner permission 98

P

- packages, file 30
- parental controls 43
- Password Assistant 51, 64
- passwords
 - authentication setup 51
 - best practices 149–151

- changing 63–65
- command-line tools 38
- firmware 21–22, 36–38, 95–96
- keychain 54
- master FileVault 104–105
- policy setup 53
- Startup Disk preferences 95–96
- tokens 52
- user 44
- vs. key-based authentication 121
- PDFs, encrypting 107–108
- permissions
 - access 16
 - disk 28–30
 - manipulating 100
 - overview 97–103
 - viewing 98
- Personal File Sharing 87
- Personal Web Sharing 128
- physical access, securing 31
- physical computers
 - hardware security 31
- PKI (public key infrastructure) 113, 115, 121
- Point-to-Point Tunneling Protocol. *See* PPTP
- portable computers
 - FileVault 104
 - keychains 57–58
 - mobile accounts 48
- portable files, encrypting 105–108
- portable keychains 57
- POSIX (Portable Operating System Interface) 29, 97–103
- PPTP (Point-to-Point Tunneling Protocol) 116
- preferences
 - accounts 63–65, 140
 - appearance 66, 140
 - Bluetooth wireless 67, 140
 - CDs 68, 141
 - checklists 139–146
 - DVDs 68, 141
 - fax 82–83, 144
 - overview 59–60
 - QuickTime 84–85, 144
 - screen saver 74–75, 142
 - See also* managed preferences
 - speech recognition 92, 145
 - time 72–73, 142
- Print & Fax preferences 82–83, 144
- Printer Sharing 87, 129
- private browsing 114
- private key 121
- privileges vs. permissions 29
- protocols. *See specific protocols*
- public key infrastructure. *See* PKI
- `pwdpolicy` command 52

Q

- QuickTime cache 84
- QuickTime preferences 84–85, 144

R

- read/write disk images 106
- recent items list 66
- Remote Apple Events 87, 129
- remote images in email 114
- remote server login 87, 120, 128
- remote system logging 134
- removable media
 - CD preferences 141
 - DVD preferences 141
 - FileVault limitations 104, 105
- root permissions 35, 46

S

- Safari preferences 114
- screen saver preferences 74–75, 85, 142
- searching preferences 93–94
- Secure Empty Trash command 110
- Secure iChat certificate 115
- secure notes 53
- secure shell. *See* SSH
- Secure Sockets Layer. *See* SSL
- Secure Transport 18
- security architecture overview 16–19
- security-mode environment variable 38
- security-password environment variable 38
- Security preferences 85–86, 144
- security server, role of 18
- Server Message Block/Common Internet File System. *See* SMB/CIFS
- servers, securing connections 124
- server-side authentication 114
- Setup Assistant 23–24
- SHA-1 digest 28
- shared resources
 - printers 82
 - user accounts 42
- share points 127
- Sharing preferences 87–90, 117, 118, 120, 127–130, 145
- single-user mode 35
- sleep mode, securing 77–78, 85
- smart cards 19, 52
- SMB/CIFS (Server Message Block/Common Internet File System) protocol 87, 128
- software, networking 113–115
- Software Update service 26–28, 90, 145
- Sound preferences 91, 145
- sparse images 106
- speech recognition preferences 92, 145
- Spotlight preferences 93–94, 146

- srm command 109–110
- SSH (secure shell host) 120–125
- ssh command 120–125
- SSL (Secure Sockets Layer) 18, 113, 115
- standard user accounts 41
- startup, securing 35–38
- Startup Disk preferences 95–96, 146
- stealth mode 117, 118
- sudo tool 46–48
- su tool 33
- su tool 46
- swap file 86
- synchronization 61–62
- syslogd configuration file 132
- system administrator (root) account 46–48
- system preferences. *See* preferences
- system setup 23–25

T

- target disk mode 96
- TCP (Transmission Control Protocol) 117
- tcpd command 119
- TCP wrappers 119
- third-party applications 45, 71, 84
- ticket-based authentication 50
- time settings 25, 72–73, 142
- TLS (Transport Layer Security) protocol
- tokens, digital 52
- Transmission Control Protocol. *See* TCP
- Transport Layer Security protocol. *See* TLS
- transport services 18
- trust services 18
- tunneling protocols, SSH 125

U

- UDP (User Datagram Protocol) 117
- UIDs (user IDs) 42–43
- Universal Access preferences 96
- UNIX and security 16
- updating software 25–28, 90
- user accounts 41–47
- User Datagram Protocol. *See* UDP
- user ID. *See* UID
- users
 - automatic actions control 68
 - home folders 48, 104–105
 - keychain management 55
 - mobile 48
 - permissions 29, 98
 - preferences control 71, 75
 - root 35
 - See also* user accounts

V

- validation, system integrity 135, 148
- virtual memory 86
- Virtual Private Network. *See* VPN
- virus screening 135
- volumes, erasing data 108
- VPN (Virtual Private Network) 115–117

W

- Web browsers 114–115
- Web sharing 87
- Windows sharing 87, 128
- wireless preferences 67

X

- Xgrid 87, 129–130