



Mac OS X Server

Security Configuration

For Mac OS X Server Version 10.6
Snow Leopard



Apple Inc.
© 2010 Apple Inc. All rights reserved.

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

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

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

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, Bonjour, FileVault, FireWire, iCal, iChat, iMac, iSight, iTunes, Keychain, Mac, Mac OS, QuickTime, Safari, Snow Leopard, Spotlight, Tiger, Time Machine, Xgrid, Xsan, and Xserve are trademarks of Apple Inc., registered in the U.S. and other countries.

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

MobileMe is a service mark of Apple Inc.

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

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

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

UNIX is a registered trademark of The Open Group.

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

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

019-1875/2010-06

Contents

Preface	17 About This Guide
	17 Audience
	17 What's in This Guide
	20 Using This Guide
	20 Using Onscreen Help
	21 Snow Leopard Server Administration Guides
	21 Viewing PDF Guides on Screen
	21 Printing PDF Guides
	22 Getting Documentation Updates
	22 Getting Additional Information
	23 Acknowledgments
Chapter 1	24 Introduction to Snow Leopard Server Security Architecture
	25 Security Architectural Overview
	25 UNIX Infrastructure
	25 Access Permissions
	26 Security Framework
	27 Layered Security Defense
	27 Network Security
	28 Credential Management
	28 Public Key Infrastructure (PKI)
	29 What's New in Snow Leopard Server Security
	29 Existing Security Features in Snow Leopard Server
	30 Signed Applications
	30 Mandatory Access Controls
	31 Sandboxing
	32 Managed User Accounts
	32 Enhanced Quarantining
	33 Memory and Runtime Protection
	33 Securing Sharing and Collaborative Services
	33 Service Access Control Lists
	34 VPN Compatibility and Integration
	35 Improved Cryptography

	35	Extended Validation Certificates
	35	Wildcard in Identity Preferences
	35	Enhanced Command-Line Tools
	36	FileVault and Encrypted Storage
	36	Encrypted Disk Image Cryptography
	36	Smart Card Support for Unlocking Encrypted Storage
	37	Enhanced Safari 4.0 Security
Chapter 2	38	Installing Snow Leopard Server
	38	Installation Overview
	39	Preparing an Administrator Computer
	40	Setting Up Network Infrastructure
	40	Starting Up for Installation
	40	Starting Up from the Install DVD
	41	Starting Up from an Alternate Partition
	41	Starting Up from a NetBoot Environment
	41	Remote Access During Installation
	42	Server Admin During Installation
	42	SSH During Installation
	42	VNC During Installation
	43	About Default Installation Passwords
	43	Preparing Disks for Installing Snow Leopard Server
	43	Securely Erasing a Disk for Installation
	44	Installing Server Software
	44	Enabling the Firewall
	45	Applying Software and Security Updates
	46	Updating from an Internal Software Update Server
	47	Updating from Internet Software Update Servers
	48	Updating Manually from Installer Packages
	50	Verifying the Integrity of Software
	50	Setting Up Services and Users
	51	About Settings Established During Server Setup
	51	Enabling the Firmware Password
Chapter 3	52	Securing System Hardware
	52	Protecting Hardware
	53	Preventing Wireless Eavesdropping
	54	Understanding Wireless Security Challenges
	54	About OS Components
	55	Removing Wi-Fi Support Software
	55	Removing Bluetooth Support Software
	56	Removing IR Support Software
	57	Preventing Unauthorized Recording

	57	Removing Audio Support Software
	58	Removing Video Recording Support Software
	59	Preventing Data Port Access
	60	Removing USB Support Software
	61	Removing FireWire Support Software
	62	System Hardware Modifications
Chapter 4	63	Securing Global System Settings
	63	Securing System Startup
	64	Using the Firmware Password Utility
	64	Using Command-Line Tools for Secure Startup
	65	Configuring Access Warnings
	66	Enabling Access Warnings for the Login Window
	67	Understanding the AuthPlugin Architecture
	68	The BannerSample Project
	69	Enabling Access Warnings for the Command Line
	70	Turning On File Extensions
Chapter 5	71	Securing Local Server Accounts
	71	Types of User Accounts
	72	Guidelines for Creating Accounts
	73	Defining User IDs
	73	Securing the Guest Account
	74	Securing Nonadministrator Accounts
	74	Securing External Accounts
	75	Protecting Data on External Volumes
	75	Securing Directory-Based Accounts
	75	Avoiding Simultaneous Local Account Access
	76	Securing Administrator Accounts
	76	About Tiered Administration Permissions
	77	Defining Administrative Permissions
	78	Avoiding Shared Administrator Accounts
	78	Securing the Directory Domain Administrator Account
	79	Changing Special Authorizations for System Functions
	79	Securing the System Administrator Account
	80	Restricting sudo Usage
	81	Understanding Directory Domains
	82	Understanding Network Services, Authentication, and Contacts
	83	Configuring LDAPv3 Access
	83	Configuring Active Directory Access
	84	Using Strong Authentication
	84	Using Password Assistant to Generate or Analyze Passwords
	85	Using Kerberos

	86	Using Smart Cards
	86	Using Tokens
	87	Using Biometrics
	87	Setting Global Password Policies
	88	Storing Credentials in Keychains
	89	Using the Default User Keychain
	89	Creating Additional Keychains
	91	Securing Keychains and Their Items
	91	Using Smart Cards as Keychains
	92	Using Portable and Network Keychains
Chapter 6	94	Securing System Preferences
	94	System Preferences Overview
	96	Securing MobileMe Preferences
	99	Securing Accounts Preferences
	102	Securing Appearance Preferences
	103	Securing Bluetooth Preferences
	105	Securing CDs & DVDs Preferences
	107	Securing Date & Time Preferences
	109	Securing Desktop & Screen Saver Preferences
	111	Securing Display Preferences
	111	Securing Dock Preferences
	112	Securing Energy Saver Preferences
	115	Securing Exposé & Spaces Preferences
	116	Securing Language & Text Preferences
	116	Securing Keyboard Preferences
	116	Securing Mouse Preferences
	117	Securing Bluetooth Settings
	117	Restricting Access to Specified Users
	118	Securing Network Preferences
	118	Disabling Unused Hardware Devices
	120	Securing Print & Fax Preferences
	122	Securing Security Preferences
	122	General Security
	123	FileVault Security
	125	Securing Sharing Preferences
	126	Securing Software Update Preferences
	128	Securing Sound Preferences
	129	Securing Speech Preferences
	130	Securing Spotlight Preferences
	133	Securing Startup Disk Preferences
	134	Securing Time Machine Preferences
	136	Securing Universal Access Preferences

Chapter 7	137 Securing System Swap and Hibernation Storage
	137 System Swap File Overview
	138 Encrypting System Swap
Chapter 8	139 Securing Data and Using Encryption
	139 About Transport Encryption
	140 About Payload Encryption
	140 About File and Folder Permissions
	141 Setting POSIX Permissions
	141 Viewing POSIX Permissions
	142 Interpreting POSIX Permissions
	143 Modifying POSIX Permissions
	143 Setting File and Folder Flags
	143 Viewing Flags
	143 Modifying Flags
	144 Setting ACL Permissions
	145 Enabling ACL Permissions
	145 Modifying ACL Permissions
	146 Changing Global Umask for Stricter Default Permissions
	147 Restricting Setuid Programs
	150 Securing User Home Folders
	151 Encrypting Home Folders
	152 Overview of FileVault
	153 Managing FileVault
	153 Managing the FileVault Master Keychain
	155 Encrypting Portable Files
	155 Creating an Encrypted Disk Image
	156 Creating an Encrypted Disk Image from Existing Data
	157 Creating Encrypted PDFs
	158 Securely Erasing Data
	158 Configuring Finder to Always Securely Erase
	159 Using Disk Utility to Securely Erase a Disk or Partition
	159 Using Command-Line Tools to Securely Erase Files
	160 Using Secure Empty Trash
	160 Using Disk Utility to Securely Erase Free Space
	161 Using Command-Line Tools to Securely Erase Free Space
	161 Deleting Permanently from Time Machine Backups
Chapter 9	163 Managing Certificates
	163 Understanding Public Key Infrastructure
	164 Public and Private Keys
	164 Certificates
	165 About Certificate Authorities (CAs)

165	About Identities
165	Self-Signed Certificates
165	About Intermediate Trust
167	Certificate Manager in Server Admin
168	Readyng Certificates
169	Creating a Self-Signed Certificate
170	Storing the Private Key
170	Requesting a Certificate from a CA
170	Creating a CA
172	Importing a Certificate Identity
173	Managing Certificates
173	Editing a Certificate
174	Distributing a CA Public Certificate to Clients
174	Deleting a Certificate
175	Renewing an Expiring Certificate
175	Replacing an Existing Certificate

Chapter 10

176	Setting General Protocols and Access to Services
176	Setting General Protocols
176	Disabling NTP Service
177	Disabling SNMP
178	Enabling SSH
178	About Remote Management (ARD)
179	Remote Management Best Practices
179	Limiting Remote Management Access
180	Disabling Remote Management Access
181	Remote Apple Events (RAE)
182	Restricting Access to Specific Users
182	Setting the Server's Host Name
182	Setting the Date and Time
183	Setting Up Certificates
183	Setting Service Access Control Lists (SACLs)

Chapter 11

185	Securing Remote Access Services
185	Securing Remote SSH Login
186	Configuring SSH
187	Modifying the SSH Configuration File
187	Generating Key Pairs for Key-Based SSH Connections
189	Updating SSH Key Fingerprints
190	Controlling Access to SSH
190	SSH Man-in-the-Middle Attacks
191	Transferring Files Using SFTP
191	Securing VPN Service

	192	VPN and Security
	193	Configuring L2TP/IPSec Settings
	194	Configuring PPTP Settings
	195	VPN Authentication Method
	196	Using VPN Service with Users in a Third-Party LDAP Domain
	196	Offering SecurID Authentication with VPN Service
	197	Encrypting Observe and Control Network Data
	197	Encrypting Network Data During File Copy and Package Installations
Chapter 12	198	Securing Network Infrastructure Services
	198	Using IPv6 Protocol
	199	IPv6-Enabled Services
	200	Securing DHCP Service
	200	Disabling Unnecessary DHCP Services
	200	Configuring DHCP Services
	201	Assigning Static IP Addresses Using DHCP
	202	Securing DNS Service
	203	Understanding BIND
	203	Turning Off Zone Transfers
	204	Disabling Recursion
	205	Preventing Some DNS Attacks
	207	Securing NAT Service
	208	Configuring Port Forwarding
	210	Disabling NAT Port Mapping Protocol
	210	Securing Bonjour (mDNS)
Chapter 13	213	Configuring the Firewall
	213	About Firewall Protection
	214	Planning Firewall Setup
	214	Configuring the Firewall Using Server Admin
	214	Starting Firewall Service
	215	Creating an IP Address Group
	216	Creating Firewall Service Rules
	217	Creating Advanced Firewall Rules
	218	Enabling Stealth Mode
	219	Viewing the Firewall Service Log
	220	Configuring the Firewall Manually
	220	Understanding IPFW Rulesets
Chapter 14	222	Securing Collaboration Services
	222	Securing iCal Service
	223	Disabling iCal Service
	223	Securely Configuring iCal Service

	225	Viewing iCal Service Logs
	225	Securing iChat Service
	225	Disabling iChat Service
	226	Securely Configuring iChat Service
	229	Viewing iChat Service Logs
	229	Securing Wiki Service
	229	Disabling Wiki Service
	230	Securely Configuring Wiki Services
	230	Viewing Wiki Service Logs
	231	Securing Podcast Producer Service
	231	Disabling Podcast Producer Service
	231	Securely Configuring Podcast Producer Service
	232	Viewing Podcast Producer Service Logs
Chapter 15	233	Securing Mail Service
	234	Disabling Mail Service
	234	Configuring Mail Service for SSL
	235	Enabling Secure Mail Transport with SSL
	235	Enabling Secure POP Authentication
	236	Configuring SSL Transport for POP Connections
	237	Enabling Secure IMAP Authentication
	237	Configuring SSL Transport for IMAP Connections
	238	Enabling Secure SMTP Authentication
	239	Configuring SSL Transport for SMTP Connections
	240	Using ACLs for Mail Service Access
	241	Limiting Junk Mail and Viruses
	241	Connection Control
	245	Filtering SMTP Connections
	245	Mail Screening
	250	Viewing Mail Service Logs
Chapter 16	251	Securing Antivirus Services
	252	Securely Configuring and Managing Antivirus Services
	252	Enabling Virus Scanning
	253	Managing ClamAV with ClamXav
	253	Viewing Antivirus Services Logs
Chapter 17	254	Securing File Services and Sharepoints
	254	Security Considerations
	254	Restricting Access to File Services
	254	Restricting Access to Everyone
	255	Restricting Access to NFS Share Points
	255	Restricting Guest Access

	255	Restricting File Permissions
	256	Protocol Security Comparison
	256	Disabling File Sharing Services
	257	Choosing a File Sharing Protocol
	258	Configuring AFP File Sharing Service
	259	Configuring FTP File Sharing Service
	262	Configuring NFS File Sharing Service
	263	Configuring SMB File Sharing Service
	264	Configuring Share Points
	265	Disabling Share Points
	265	Restricting Access to a Share Point
	267	AFP Share Points
	267	SMB Share Points
	268	FTP Share Points
	268	NFS Share Points
Chapter 18	271	Securing Web Service
	272	Disabling Web Service
	272	Managing Web Modules
	273	Disabling Web Options
	274	Using Realms to Control Access
	276	Enabling Secure Sockets Layer (SSL)
	278	Using a Passphrase with SSL Certificates
	278	Viewing Web Service Logs
	279	Securing WebDAV
	280	Securing Blog Services
	280	Disabling Blog Services
	280	Securely Configuring Blog Services
	281	Securing Tomcat
	282	Securing MySQL
	282	Disabling MySQL Service
	282	Setting Up MySQL Service
	283	Viewing MySQL Service and Admin Logs
Chapter 19	284	Securing Client Configuration Management Services
	284	Managing Applications Preferences
	285	Controlling User Access to Applications and Folders
	287	Allowing Specific Dashboard Widgets
	288	Disabling Front Row
	289	Allowing Legacy Users to Open Applications and Folders
	291	Managing Dock Preferences
	292	Managing Energy Saver Preferences
	293	Managing Finder Preferences

	295	Managing Login Preferences
	298	Managing Media Access Preferences
	299	Managing Mobility Preferences
	301	Managing Network Preferences
	302	Managing Parental Controls Preferences
	303	Hiding Profanity in Dictionary
	303	Preventing Access to Adult Websites
	304	Allowing Access Only to Specific Websites
	306	Setting Time Limits and Curfews on Computer Usage
	307	Managing Printing Preferences
	308	Managing Software Update Preferences
	308	Managing Access to System Preferences
	309	Managing Universal Access Preferences
	310	Enforcing Policy
Chapter 20	311	Securing NetBoot Service
	311	Securing NetBoot Service
	311	Disabling NetBoot Service
	312	Limit NetBoot Service Clients
	314	Viewing NetBoot Service Logs
Chapter 21	315	Securing Software Update Service
	315	Disabling Software Update Service
	316	Limiting Automatic Update Availability
	317	Viewing Software Update Service Logs
Chapter 22	318	Securing Network Accounts
	318	About Open Directory and Active Directory
	319	Securing Directory Accounts
	319	Configuring Directory User Accounts
	321	Configuring Group Accounts
	322	Configuring Computer Groups
	323	Controlling Network Views
Chapter 23	324	Securing Directory Services
	325	Open Directory Server Roles
	325	Configuring the Open Directory Services Role
	326	Starting Kerberos After Setting Up an Open Directory Master
	327	Configuring Open Directory for SSL
	329	Configuring Open Directory Policies
	329	Setting the Global Password Policy
	330	Setting a Binding Policy for an Open Directory Master and Replicas
	331	Setting a Security Policy for an Open Directory Master and Replicas

Chapter 24	333	Securing RADIUS
	333	Disabling RADIUS
	334	Securely Configuring RADIUS Service
	334	Configuring RADIUS to Use Certificates
	335	Editing RADIUS Access
	335	Viewing RADIUS Service Logs
Chapter 25	337	Securing Print Service
	337	Disabling Print Service
	338	Securing Print Service
	338	Configuring Print Service Access Control Lists (SACLs)
	339	Configuring Kerberos
	340	Configuring Print Queues
	342	Viewing Print Service and Queue Logs
Chapter 26	344	Securing Multimedia Services
	344	Disabling QTSS
	345	Securely Configuring QTSS
	346	Configuring a Streaming Server
	347	Serving Streams Through Firewalls Using Port 80
	347	Streaming Through Firewalls or Networks with Address Translation
	348	Changing the Password Required to Send an MP3 Broadcast Stream
	348	Using Automatic Unicast (Announce) with QTSS on a Separate Computer
	349	Controlling Access to Streamed Media
	353	Viewing QTSS Logs
Chapter 27	354	Securing Grid and Cluster Computing Services
	354	Understanding Xgrid Service
	355	Disabling Xgrid Service
	355	About Authentication Methods for Xgrid
	356	Single Sign-On
	356	Password-Based Authentication
	357	No Authentication
	357	Securely Configuring Xgrid Service
	357	Disabling the Xgrid Agent
	358	Limiting the Xgrid Agent
	359	Configuring an Xgrid Controller
Chapter 28	361	Managing Who Can Obtain Administrative Privileges (sudo)
	361	Managing the sudoers File
Chapter 29	363	Managing Authorization Through Rights
	363	Understanding the Policy Database
	363	The Rights Dictionary

	365	Rules
	366	Managing Authorization Rights
	366	Creating an Authorization Right
	366	Modifying an Authorization Right
	366	Example Authorization Restrictions
Chapter 30	368	Maintaining System Integrity
	368	Using Digital Signatures to Validate Applications and Processes
	369	Validating Application Bundle Integrity
	370	Validating Running Processes
	370	Auditing System Activity
	370	Installing Auditing Tools
	371	Enabling Auditing
	372	Setting Audit Mechanisms
	372	Using Auditing Tools
	372	Using the audit Tool
	373	Using the auditreduce Tool
	374	Using the praudit Tool
	375	Deleting Audit Records
	375	Audit Control Files
	376	Managing and Analyzing Audit Log Files
	376	Using Activity Analysis Tools
	377	Validating System Logging
	377	Configuring syslogd
	378	Local System Logging
	378	Remote System Logging
	379	Viewing Logs in Server Admin
Appendix A	380	Understanding Passwords and Authentication
	380	Password Types
	380	Authentication and Authorization
	381	Open Directory Passwords
	382	Shadow Passwords
	382	Crypt Passwords
	382	Offline Attacks on Passwords
	383	Password Guidelines
	383	Creating Complex Passwords
	383	Using an Algorithm to Create a Complex Password
	384	Safely Storing Your Password
	385	Password Maintenance
	385	Authentication Services
	386	Determining Which Authentication Option to Use
	387	Password Policies

387	Single Sign-On Authentication
388	Kerberos Authentication
389	Smart Card Authentication
Appendix B	
390	Security Checklist
390	Installation Action Items
391	Hardware and Core Snow Leopard Server Action Items
391	Global Settings for Snow Leopard Server Action Items
392	Account Configuration Action Items
393	System Software Action Items
393	MobileMe Preferences Action Items
393	Accounts Preferences Action Items
393	Appearance Preferences Action Items
394	Bluetooth Preferences Action Items
394	CDs & DVDs Preferences Actions Items
394	Exposé & Spaces Preferences Action Items
394	Date & Time Preferences Action Items
395	Desktop & Screen Saver Preferences Action Items
395	Display Preferences Action Items
395	Dock Preferences Action Items
395	Energy Saver Preferences Action Items
396	Keyboard and Mouse Preferences Action Items
396	Network Preferences Action Items
396	Print & Fax Preferences Action Items
396	QuickTime Preferences Action Items
397	Security Preferences Action Items
397	Sharing Preferences Action Items
397	Software Update Preferences Action Items
397	Sound Preferences Action Items
398	Speech Preferences Action Items
398	Spotlight Preferences Action Items
398	Startup Disk Preferences Action Items
398	Time Machine Preferences Action Items
398	Data Maintenance and Encryption Action Items
399	Account Policies Action Items
399	Share Points Action Items
399	Account Configuration Action Items
400	Applications Preferences Action Items
400	Dock Preferences Action Items
401	Energy Saver Preferences Action Items
401	Finder Preferences Action Items
401	Login Preferences Action Items
402	Media Access Preferences Action Items

403	Mobility Preferences Action Items
403	Network Preferences Action Items
403	Printing Preferences Action Items
404	Software Update Preferences Action Items
404	Access to System Preferences Action Items
404	Universal Access Preferences Action Items
405	Certificates Action Items
405	General Protocols and Service Access Action Items
405	Remote Access Services Action Items
407	Network and Host Access Services Action Items
407	IPv6 Protocol Action Items
407	DHCP Service Action Items
407	DNS Service Action Items
408	Firewall Service Action Items
408	NAT Service Action Items
408	Bonjour Service Action Items
408	Collaboration Services Action Items
409	Mail Service Action Items
410	File Services Action Items
410	AFP File Sharing Service Action Items
410	FTP File Sharing Service Action Items
411	NFS File Sharing Service Action Items
411	SMB Action Items
412	Web Service Action Items
412	Client Configuration Management Services Action Items
412	Directory Services Action Items
413	Print Service Action Items
413	Multimedia Services Action Items
413	Grid and Cluster Computing Services Action Items
414	Validating System Integrity Action Items
Appendix C	415 Scripts
Index	445

About This Guide

Use this guide as an overview of Mac OS X v10.6 Snow Leopard Server security features that can enhance security on your computer.

This guide gives instructions for securing Snow Leopard Server, and for securely managing servers and clients in a networked environment. It also provides information about the many roles Snow Leopard Server can assume in a network.

Audience

Administrators of server computers running Snow Leopard Server are the intended audience for this guide.

If you're using this guide, you should be an experienced Snow Leopard Server user, be familiar with the Workgroup Manager and Server Admin applications, and have at least some experience using the Terminal application's command-line interface.

You should also have experience administering a network, be familiar with basic networking concepts, and be familiar with the Snow Leopard Server administration guides.

Some instructions in this guide are complex, and deviation from them could result in serious adverse effects on the server and its security. These instructions should only be used by experienced Snow Leopard Server administrators, and should be followed by thorough testing.

What's in This Guide

This guide explains how to secure servers and securely manage server and client computers in a networked environment. It does not provide information about securing clients. For help with securing computers running Snow Leopard, see *Mac OS X Security Configuration*.

This guide cannot cover all possible network configurations in which Snow Leopard Server might be used. Good network security and design must be used for this information to be effective, and anyone using this guide needs to be familiar with UNIX security basics, such as setting file permissions.

This guide includes the following chapters, arranged in the order that you're likely to need them when securely configuring a server.

- Chapter 1, "Introduction to Snow Leopard Server Security Architecture," provides an overview of the security architecture and features of Snow Leopard Server. This chapter describes the security framework, access permissions, built-in security services, and directory services.
- Chapter 2, "Installing Snow Leopard Server," describes how to securely install Snow Leopard Server locally or remotely. This chapter also includes information about updating system software, repairing disk permissions, and securely erasing data.
- Chapter 3, "Securing System Hardware," describes how to physically protect your hardware from attacks.
- Chapter 4, "Securing Global System Settings," describes how to secure settings that affect all users of the computer.
- Chapter 5, "Securing Local Server Accounts," describes the types of user accounts and how to securely configure an account. This includes securing accounts using strong authentication.
- Chapter 6, "Securing System Preferences," helps you configure local server accounts securely. This includes the secure configuration of local system preferences, setting up strong authentication and credential storage, and securing data.
- Chapter 7, "Securing System Swap and Hibernation Storage," describes how to scrub your system swap and hibernation space of sensitive information.
- Chapter 8, "Securing Data and Using Encryption," describes how to encrypt data and how to use Secure Erase to ensure old data is completely removed.
- Chapter 9, "Managing Certificates," describes how to generate, request, and deploy certificates.
- Chapter 10, "Setting General Protocols and Access to Services," helps you configure general network management protocols and restrict access to other services.
- Chapter 11, "Securing Remote Access Services," tells you how to create remote connections to your server using encryption.
- Chapter 12, "Securing Network Infrastructure Services," explains how to connect client computers and configure a firewall.
- Chapter 13, "Configuring the Firewall," describes how to configure the IPFW2 firewall.
- Chapter 14, "Securing Collaboration Services," describes how to securely configure iChat, iCal, Wiki, and Podcast Producer services.
- Chapter 15, "Securing Mail Service," explains how to set up mail service to use encryption and filter for spam and viruses.
- Chapter 16, "Securing Antivirus Services," describes how to enable and manage antivirus services to protect your mail and files.

- Chapter 17, “Securing File Services and Sharepoints,” explains how to configure file services to enable secure data sharing.
- Chapter 18, “Securing Web Service,” describes how to set up a web server and secure web settings and components.
- Chapter 19, “Securing Client Configuration Management Services,” helps you set policies and enforce them using Workgroup Manager.
- Chapter 20, “Securing NetBoot Service,” tells you how to configure NetBoot securely to provide images to clients.
- Chapter 21, “Securing Software Update Service,” describes how to securely configure software update services.
- Chapter 22, “Securing Network Accounts,” describes security settings related to managed user and group accounts.
- Chapter 23, “Securing Directory Services,” explains how to configure Open Directory service roles and password policies.
- Chapter 24, “Securing RADIUS,” tells how to securely configure RADIUS.
- Chapter 25, “Securing Print Service,” explains how to set up print queues and banner pages.
- Chapter 26, “Securing Multimedia Services,” provides security information to configure a streaming server.
- Chapter 27, “Securing Grid and Cluster Computing Services,” explains how to securely configure an Xgrid agent and controller.
- Chapter 28, “Managing Who Can Obtain Administrative Privileges (`sudo`),” describes how to restrict access to the `sudo` command.
- Chapter 29, “Managing Authorization Through Rights,” explains the policy database and how to control authorization by managing rights in the policy database.
- Chapter 30, “Maintaining System Integrity,” describes how to use security audits and logging to validate the integrity of your server and data.
- Appendix A, “Understanding Passwords and Authentication,” describes Open Directory authentication, shadow and crypt passwords, Kerberos, LDAP bind, and single sign-on.
- Appendix B, “Security Checklist,” provides a checklist that guides you through securing your server.
- Appendix C, “Scripts,” provides command-line commands and scripts for securing your server.

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 list contains suggestions for using this guide:

- Read the guide in its entirety. Subsequent sections might build on information and recommendations discussed in prior sections.
- The instructions in this guide should always be tested in a nonoperational environment before deployment. This nonoperational environment should simulate, as much as possible, the environment where the computer will be deployed.
- This information is intended for computers running Snow Leopard Server. Before securely configuring a server, determine what function that particular server will perform and apply security configurations where applicable.
- Use the security checklist in Appendix B to track and record each security task and note what settings you changed. 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. Take measures to monitor or mitigate those risks.

Using Onscreen Help

You can get task instructions onscreen in Help Viewer while you're managing Snow Leopard Server. You can view help on a server or an administrator computer. (An administrator computer is a computer running Snow Leopard Server with the server administration tools installed)

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

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

The onscreen help contains instructions taken from the advanced administration guides described in "Snow Leopard Server Administration Guides," next.

To see the most recent server help topics:

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

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

Snow Leopard Server Administration Guides

Getting Started covers installation and setup for standard and workgroup configurations of Snow Leopard Server. For advanced configurations, *Advanced Server Administration* covers planning, installation, setup, and general server administration.

A suite of additional guides covers advanced planning, setup, and management of individual services. You can get these guides in PDF format from the Snow Leopard Server documentation website:

www.apple.com/server/macosx/resources/documentation.html

Viewing PDF Guides on Screen

While reading the PDF version of a guide onscreen:

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

Printing PDF Guides

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

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

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

Getting Documentation Updates

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

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

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—get important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx)—enter the gateway to extensive product and technology information.
- *Snow Leopard Server Support website* (www.apple.com/support/macosxserver)—access hundreds of articles from Apple’s support organization.
- *Apple Discussions website* (discussions.apple.com)—share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Training and Certification website* (www.apple.com/training)—hone your server administration skills with instructor-led or self-paced training, and differentiate yourself with certification.
- *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/darwin/)—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 (NSA) provides information about securely configuring proprietary and open source software.
- *NIST Security Configuration Checklists Repository* (checklists.nist.gov/repository/category.html)—This is the National Institute of Standards and Technology (NIST) repository for security configuration checklists.
- *DISA Security Technical Implementation Guide* (www.disa.mil/gs/dsn/policies.html)—This is the Defense Information Systems Agency (DISA) 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)—This is the Center for Internet Security (CIS) benchmark and scoring tool used to establish CIS benchmarks.

Acknowledgments

Apple would like to thank the NSA, NIST, and DISA for their assistance in contributing to the security configuration guides for Snow Leopard and Snow Leopard Server.

Introduction to Snow Leopard Server Security Architecture

Use this chapter to learn about the features in Snow Leopard Server that can enhance security on your computer

Whether you're a home user with a broadband Internet connection, a professional with a mobile computer, or an IT manager with thousands of networked systems, you need to safeguard the confidentiality of information and the integrity of your computers.

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

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

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

Security Architectural Overview

Snow Leopard Server security services are built on two open source standards:

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

UNIX Infrastructure

The Snow Leopard Server kernel—the heart of the operating system—is built from BSD and Mach.

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

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

Access Permissions

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

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

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

Authorization Versus Authentication

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

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

Security Framework

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

The CDSA code is used by Snow Leopard features such as Keychain and URL Access for protection of login data.

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

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

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

Layered Security Defense

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



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

Network Security

Secure Transport is used to implement SSL and Transport Layer Security (TLS) protocols. These protocols provide secure communications over a TCP/IP connection such as the Internet by using encryption and certificate exchange. A firewall can then filter communication over a TCP/IP connection by permitting or denying access to a computer or a network.

Credential Management

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

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

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

Public Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) includes certificate, key, and trust services include functions to:

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

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

What's New in Snow Leopard Server Security

Snow Leopard Server offers the following major security enhancements:

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

Existing Security Features in Snow Leopard Server

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

- **Application signing:** This enables you to verify the integrity and identity of applications on your Mac.
- **Mandatory access control:** These enforce restrictions on access to system resources.
- **Quarantined applications:** Mac OS X v10.6 tags and marks downloaded files with first-run warnings to help prevent users from inadvertently running malicious downloaded applications.
- **Runtime protection:** Technologies such as execute disable, library randomization, and sandboxing help prevent attacks that try to hijack or modify the software on your system.

- **Meaningful security alerts:** When users receive security alerts and questions too frequently, they may fall into reflexive mode when the system asks a security-related question, clicking OK without thought. Mac OS X v10.6 minimizes the number of security alerts that you see, so when you do see one, it gets your attention.

Signed Applications

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

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

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

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

Mandatory Access Controls

Snow Leopard Server uses an access control mechanism known as mandatory access controls. Although the Mandatory Access Control technology is not visible to users, it is included in Snow Leopard Server to protect your computer.

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

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

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

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

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

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

Sandboxing

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

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

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

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

Managed User Accounts

Parental controls provide computer administrators with the tools to enforce a reasonable level of restrictions for users of the computer.

Administrator users can use features like Simple Finder to limit the launching of a set of applications or create a white list of web sites that users can visit. However, if an attacker has physical access to the computer ports such as USB or FireWire, Parental controls can be bypassed by mounting a disk image that contain malicious software.

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

This is the kind of simple UI administrators of a public use computer environment can use to restrict access to applications or sites to keep users from performing malicious activities. It is not a fool-proof security system for local users.

In Snow Leopard Server, you use Workgroup Manager to manage preferences for users of Snow Leopard systems.

Enhanced Quarantining

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

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

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

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

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

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

Memory and Runtime Protection

Snow Leopard Server running on a 64-bit chip supports memory and executable protection. Memory execution prevention works to hinder specific types of malicious software, those that rely on executing arbitrary code from an area which expected to contain data and not code.

Snow Leopard has the following 64-bit protection features: no-execute stack, noexecute data, and no-execute heap. In Snow Leopard, no-execute stack is available for 32- and 64-bit applications. For 64-bit processes, Snow Leopard provides protection from code execution in both heap and stack data areas. Stack protection is available for both 32-bit and 64-bit processes. It detects certain cases of stack memory corruption which could lead to arbitrary code execution and terminates the process.

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

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

Securing Sharing and Collaborative Services

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

Service Access Control Lists

You can further secure sharing services by allowing access only to users that you specified in a service access control lists (SACLs). You can create user accounts for sharing based on existing user accounts on the system, and for entries in your address book. Sharing services become more secure with SACLs.

VPN Compatibility and Integration

Snow Leopard Server supports standards-based L2TP/IPSec and PPTP tunneling protocols to provide encrypted VPN connections for Mac and Windows systems — and even iPhone. These VPN services use secure authentication methods, including MS-CHAPv2 and network-layer IPSec. In addition, the L2TP VPN server can authenticate users using credentials from a Kerberos server.

To use VPN service for users in a third-party LDAP domain (an Active Directory or Linux OpenLDAP domain), you must be able to use Kerberos authentication. If you need to use MSCHAPv2 to authenticate users, you can't offer VPN service for users in a third-party LDAP domain.

Apple's VPN server can authenticate using RSA Security's SecurID. This provides strong two-factor authentication. It uses hardware and software tokens to verify user identity. However, SecurID authentication cannot be set up from Server Admin and requires additional manual setup.

Built-in VPN Client

In Snow Leopard, the VPN client built into Network Preferences includes support for Cisco Group Filtering and DHCP over PPP to dynamically acquire additional configuration options such as static routes and search domains.

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

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

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

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

Improved Cryptography

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

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

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

Extended Validation Certificates

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

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

Wildcard in Identity Preferences

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

This is often used with certificates used by Common Access Cards (CACs). For more information on Smart Cards, see "Smart Card Support for Unlocking Encrypted Storage" on page 36.

Enhanced Command-Line Tools

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

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

FileVault and Encrypted Storage

The Disk Utility tool included in Mac OS X enables you to create encrypted disk images, so you can safely mail valuable documents, files, and folders to friends and colleagues, save the encrypted disk image to CD or DVD, or store it on the local system or a network file server.

FileVault also uses this same encrypted disk image technology to protect user folders.

Encrypted Disk Image Cryptography

A disk image is a file that appears as a volume on your hard disk. It can be copied, moved, or opened. When the disk image is encrypted, files or folders placed in it are encrypted using 128-bit or even stronger 256-bit AES encryption.

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

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

Smart Card Support for Unlocking Encrypted Storage

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

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

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

Other commercial smart card vendors provide token modules to support integration of their smart card with the Snow Leopard Smart Card architecture.

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

Snow Leopard Server has additional functionality for smart card use, such as:

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

Enhanced Safari 4.0 Security

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

Safari also includes a fraudulent site detection feature. It works like this:

Google maintains a blacklist of known and highly-suspected malware-transmitting sites and “phishing” sites (harvesters of sensitive data). Google adds a hash of each site’s URL to a database that some web browsers can use at safebrowsing.clients.google.com.

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

Safari stores the data in the folder at /private/var/folders/ in folders with two-letter names. The full path is /private/var/folders/xx/yy/-Caches-/com.apple.Safari, where “xx” and “yy” are unique codes. When you find that folder, you’ll see two files: Cache.db and SafeBrowsing.db.

Installing Snow Leopard Server

2

Use this chapter to customize the default installation of Snow Leopard Server for your specific network security needs.

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

Important: When possible, computers should remain isolated from the operational network until they are completely and securely configured. Use an isolated test network for installation and configuration.

Installation Overview

Detailed instructions for Snow Leopard Server Installation are found in the *Advanced Server Administration* guide. This section contains basic practices consistent with a secure installation of Snow Leopard Server.

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

Because some recoverable data might remain on the computer, securely erase the partition you're installing Snow Leopard Server on. For more information, see "Securely Erasing a Disk for Installation" on page 43.

If you decide against securely erasing the partition, securely erase free space after installing Snow Leopard Server. For more information, see "Using Disk Utility to Securely Erase Free Space" on page 160.

There are several ways to install the operating system, depending on your environment and installation strategy. In general, all installations have a few common steps:

- Prepare an administrator computer.
- Set up network infrastructure.
- Start up from a disk other than the target volume (for example, the Installation Disc).
- Prepare the target disk.
- Start the installation via Server Assistant, command line, or VNC.
- Enable the firewall, blocking all incoming connections.
- Apply software updates and security updates.
- Configure the server and set up services.
- Enable the Firmware Password.

Preparing an Administrator Computer

You can use an administrator computer to install, set up, and administer Snow Leopard Server on another computer. An administrator computer is a computer with Snow Leopard Server or Snow Leopard that you use to manage remote servers.

You cannot run the server administration tools from a Leopard or Leopard Server computer.

When you install and set up Snow Leopard Server on a computer that has a display and keyboard, it's already an administrator computer. To make a computer with Snow Leopard into an administrator computer, you must install additional software.

Important: If you have administrative applications and tools from Leopard Server or earlier, do not use them with Snow Leopard Server.

To install Snow Leopard Server administration tools:

- 1 Make sure the computer has Snow Leopard installed.
- 2 Make sure the computer has at least 1 GB of RAM and 1 GB of unused disk space.
- 3 Insert the Mac OS X Server Install Disc.
- 4 Open the Other Installers folder.
- 5 Open serveradministrationSoftware.mpkg to start the Installer and then follow the onscreen instructions.

Setting Up Network Infrastructure

Before you can install, you must set up or have the following settings for your network service:

- **DNS:** You must have a fully qualified domain name for each server's IP address in the DNS system. The DNS zone must have the reverse-lookup record for the name and address pair. Not having a stable, functioning DNS system with reverse lookup leads to service failures and unexpected behaviors.
- **Static IP Address:** Make sure you already have a static IP address planned and assigned to the server.
- **DHCP:** Do not assign dynamic IP addresses to servers. If your server gets its IP address through DHCP, set up a static mapping in the DHCP server so your server gets (via its Ethernet address) the same IP address every time.
- **Firewall or routing:** In addition to any firewall running on your server, the subnet router might have specific network traffic restrictions in place. Make sure the server's IP address is available for the traffic it will handle and the services you will run.

Starting Up for Installation

The computer can't install to its own startup volume, so you must start up in some other way, such as:

- The Installation DVD
- Alternate volumes (second partitions on the hard disk or external FireWire disks)
For information on using alternate volumes, see the *Advanced Server Administration* guide.
- NetBoot (if the network and NetBoot servers are trusted)
For information on using NetBoot servers, see the *System Imaging and Software Update Administration* guide.

Starting Up from the Install DVD

The computer must install from the same disk or image that started up the computer. Mounting another share point with an installer won't work. The installer uses some of the files active in the booted system partition for the new installation.

The easiest and most secure way to install Snow Leopard Server is to install it physically at the computer, known as a local installation, using the DVD. When performing a local installation, it is recommended, if applicable, that the entire drive be reformatted using at least a 7-pass secure erase, rather than only reformatting the partition where Snow Leopard Server is to be installed, in case sensitive information was left on the other partitions.

If the target server is an Xserve with a built-in DVD drive, start the server using the Install DVD by following the instructions in the *Xserve User's Guide* for starting from a system disc.

Starting Up from an Alternate Partition

For a single-server installation, preparing to start up from an alternate partition can be more time-consuming than using the Install DVD. The time required to image, scan, and restore the image to a startup partition can exceed the time taken to install once from the DVD.

However, if you are reinstalling regularly, or if you are creating an external FireWire drive-based installation to take to various computers, or if you need some other kind of mass distribution (such as clustered Xserves without DVD drives installed), this method can be very efficient.

Note: When creating a bootable external disk, use the GUID Partitioning format.

Starting Up from a NetBoot Environment

If you have an existing NetBoot infrastructure, this is the easiest way to perform mass installation and deployment. This method can be used for clusters that have no optical drive or existing system software.

This method can also be used in environments where large numbers of servers must be deployed in an efficient manner.

This section won't tell you how to create the necessary NetBoot infrastructure. If you want to set up NetBoot and NetInstall options for your network, servers, and client computers, see the manuals at www.apple.com/server/resources/.

Remote Access During Installation

Snow Leopard Server has several remote access services active during installation. It provides Server Admin administration, SSH access and VNC access when starting from the installation disk.

Important: Before you install or reinstall Snow Leopard Server, make sure the network is secure because remote access technologies can potentially give others access to the computer over the network. For example, design the network topology so you can make the server computer's subnet accessible only to trusted users.

Server Admin During Installation

A computer that started up from the installation disc broadcasts its installation availability via Bonjour to the local network. You can find servers that are awaiting install by finding the Bonjour service name “_sa-rspnldr._tcp.”

You can use the dns-sd tool to identify computers on the local subnet where you can install server software. Enter the following from a computer on the same local network as the server:

```
dns-sd -B _sa-rspnldr._tcp.
```

Administrator computers running Server Admin’s Server Assistant can provide a default password and complete installation remotely. Server Admin traffic is encrypted.

SSH During Installation

When you start up a computer from a server installation disc, SSH starts so that remote installations can be performed via the command line. SSH service is granted to the root user providing the default password.

VNC During Installation

VNC enables you to use a VNC viewer (like Screen Sharing or Apple Remote Desktop) to view the user interface as if you were using the remote computer’s keyboard, mouse, and monitor.

All the things you can do at the computer using the keyboard and mouse are available remotely, as well as locally. This excludes hardware restarts (using the power button to shut down and restart the computer), other hardware manipulation, or holding down keys during startup. VNC viewers are available for all popular computing platforms.

VNC traffic is not secure without additional precautions. Establish an SSH tunnel between the local host and the remote server to securely perform the installation by redirecting the VNC traffic through the tunnel.

For example, to redirect Apple Remote Desktop traffic through an SSH tunnel, enter:

```
ssh -v -L 2501:local_host:5900 target_server -l target_server_username
```

About Default Installation Passwords

Server serial numbers are used for more than inventory tracking. The server's built-in hardware serial number is used as the default password for remote installation.

The password is case sensitive.

To find a server's serial number, look for a label on the server. If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

If you replace a main logic board on an Intel Xserve, the built-in hardware password is "System S" (no quotes).

Preparing Disks for Installing Snow Leopard Server

Before performing a clean installation of Snow Leopard Server, you can partition the server computer's hard disk into multiple volumes, create a RAID set, or erase the target disk or partition.

If you're using an installation disc for Snow Leopard Server or later, you can perform these tasks from another networked computer using VNC viewer software, such as Apple Remote Desktop, before beginning a clean installation.

WARNING: Before partitioning a disk, creating a RAID set, or erasing a disk or partition on a server, preserve user data you want to save by copying it to another disk or partition.

Securely Erasing a Disk for Installation

When performing an installation, it is recommended, if applicable, that the entire drive be reformatted using at least a 7-pass secure erase, rather than only reformatting the partition where Snow Leopard Server is to be installed, in case sensitive information was left on the other partitions.

You have several options for erasing a disk, depending on your preferred tools and your computing environment:

- **Erasing a disk using Disk Utility:** You can use the Installer to open Disk Utility and then use it to erase the target volume or another volume. You can erase the target and all other volumes using the Mac OS Extended format or Mac OS Extended (Journaled) format. You can erase other volumes using those formats, as well as Mac OS Extended format (Case-Sensitive) format, or Mac OS Extended (Journaled, Case-Sensitive) format.

You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Mac computer with Mac OS X v10.6 and choose Help > Disk Utility Help.

- **Erasing a disk using the command line:** You can use the command line to erase disks using the tool `diskutil`. Erasing a disk using `diskutil` results in losing all volume partitions. The command to erase a complete disk is:

```
sudo diskutil secureErase 2 format name device
```

For example:

```
sudo diskutil secureErase 2 JournaledHFS+ MacProHD disk0
```

There is also an option to securely delete data by overwriting the disk with random data multiple times. For more details, see `diskutil`'s man page.

To erase a single volume on a disk, a slightly different command is used:

```
diskutil eraseVolume format name device
```

For example:

```
diskutil eraseVolume JournaledHFS+ UntitledPartition /Volumes/  
OriginalPartition
```

For complete command syntax for `diskutil`, consult the tool's man page.

Installing Server Software

When the target computer is started, you use Server Admin's Server Assistant (locally or remotely), VNC control, or the `installer` command-line tool to start installation.

For detailed instructions on using one of these methods to install Snow Leopard Server, see the *Advanced Server Administration* guide.

Enabling the Firewall

After configuration, enable the firewall to prevent unauthorized connections to the server while you complete setup. For a more comprehensive treatment of firewall configuration, see Chapter 13, "Configuring the Firewall."

When running, the default firewall configuration on Snow Leopard Server denies access to incoming packets from remote computers except through ports for remote configuration. This provides a high level of security.

Stateful rules are in place as well, so responses to outgoing queries initiated by your computer are also permitted. You can then add rules to permit server access to clients who require access to services.

Important: Use great care in remotely changing any firewall configuration because of the risk of disabling communications to the remote host.

To enable the firewall:

- 1 Open Server Admin and connect to the server.
- 2 Click the triangle at the left of the server.
The list of services appears.
- 3 From the expanded Servers list, select Firewall.

If Firewall is not listed as an available service to configure, add it to the server view by doing the following:

- a In the server list on the left, select the server name.
 - b Click the Settings button in the toolbar and then click the Services tab.
 - c Select the checkbox for Firewall service.
- 4 Click the Start Firewall button below the Servers list.

From the command line:

```
# -----
# Securing Firewall Service
# -----
#
# Add Firewall to the services view
# -----
sudo serveradmin settings
    info:serviceConfig:services:com.apple.ServerAdmin.ipfilter:configured
        = yes
# Start Firewall service
# -----
sudo serveradmin start ipfilter
```

Applying Software and Security Updates

After installing Snow Leopard Server, install the latest approved security updates.

Before connecting your computer to a network to obtain software updates, enable the firewall using Server Admin to allow only essential services.

Important: If you have not secured and validated settings for network services, do not enable your network connection to install software updates. For information, see “Securing Network Infrastructure Services” on page 198.

Until you securely configure network services settings, limit your update installation to using the manual method of installing software updates. For more information, see “Updating Manually from Installer Packages” on page 48.

Snow Leopard Server includes Software Update, an application that downloads and installs software updates from Apple's Software Update server or from an internal software update server.

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

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

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

Software updates are obtained and installed in several ways:

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

Updating from an Internal Software Update Server

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

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

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

From the command line:

```
#  
# Updating from an Internal Software Update Server  
# -----  
# Default Settings.  
# blank  
# Software updates are downloaded from one of the following software update  
# servers hosted by Apple.  
# swscan.apple.com:80  
# swquery.apple.com:80  
# swcdn.apple.com:80  
  
# Suggested Settings.  
# Specify the software update server to use.  
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate  
    CatalogURL http://swupdate.apple.com:8088/index-leopard-  
    snowleopard.merged-1.sucatalog  
  
# Available Settings.  
# Replace swupdate.apple.com with the fully qualified domain name (FQDN)  
# or IP address of your software update server.  
  
# To switch your computer back to the default Apple update server.  
# sudo defaults delete com.apple.SoftwareUpdate CatalogURL
```

Updating from Internet Software Update Servers

Before connecting to the Internet, make sure your network services are securely configured. For information, see “Securing Network Infrastructure Services” on page 198.

If you are a network administrator, instead of using your operational computer to check for and install updates, consider using a test computer to download updates and verify file integrity before installing updates. For more information about verifying file integrity, see “Verifying the Integrity of Software” on page 50.

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 48.

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

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

To download and install software updates using Software Update:

- 1 Choose Apple (apple) > Software Update.

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

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

When you keep the package, it is stored in the user's Downloads folder (*user_name/Downloads/*).

If you do not want to install updates, click Quit.

- 3 Accept the licensing agreements to start installation.

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

From the command line:

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

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

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

Updating Manually from Installer Packages

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

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

To manually download, verify, and install software updates:

- 1 Go to support.apple.com/downloads/ and download the software updates on a computer designated for verifying software updates.
- Note:** Updates provided through Software Update might sometimes appear earlier than standalone updates.
- 2 For each update file downloaded, review the SHA-1 digest (also known as a checksum), which should be posted online with the update package.
- 3 Inspect downloaded updates for viruses.
- 4 Verify the integrity of each update.
For more information, see “Verifying the Integrity of Software” on page 50.
- 5 Transfer the update packages from your test computer to your current computer.
The default download location for update packages is /Library/Updates/. You can transfer update packages to any location on your computer.
- 6 Double-click the package.
If the package is located in a disk image (dmg) file, double-click the dmg file and then double-click the package.
- 7 Proceed through the installation steps.
- 8 If requested, restart the computer.

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

From the command line:

```
# Updating Manually from Installer Packages
# -----
# Default Settings.
# None

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

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

Verifying the Integrity of Software

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

From the command line:

```
# Verifying the Integrity of Software
# -----
# Default Settings.
# None

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

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

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

Setting Up Services and Users

After installation, the server is ready for configuration and local administrator account creation.

An unconfigured server broadcasts its installation availability via Bonjour to the local network. You can find servers that are awaiting install by finding the Bonjour service name “_svr-unconfig._tcp.”

The easiest way of finding a server that needs configuration is by using the tools installed on the administration computer: Server Admin or Server Preferences.

These tools can detect servers waiting configuration on the local subnet, available via Bonjour.

If you are trying to find servers awaiting configuration using the command line, you can use the dns-sd tool to identify computers on the local subnet where you can install server software. Enter the following from a computer on the same local network as the server:

```
dns-sd -B _sa-unconfig._tcp.
```

Administrator computers running Server Admin's Server Assistant can provide a default password and complete installation remotely. Server Admin traffic is encrypted.

In either case, the login name and password are described in the section "About Default Installation Passwords" on page 43.

About Settings Established During Server Setup

During server setup, the following basic server settings are established:

- The language to use for server administration and the computer keyboard layout is defined.
- The server software serial number is set.
- A time zone is specified, and network time service is set up.
- A server administrator local user is defined and the local administrator's home folder is created.
- The default SSH and Apple Remote Desktop state is enabled.
- Network interfaces (ports) are configured.

TCP/IP and Ethernet settings are defined for each port you want to activate.

- Network names are defined.

The primary DNS name and computer name are defined by the administrator, and the local hostname is derived from the computer name.

- Basic Directory information is set up. (Optional)

The server is set up as an Open Directory Master, or it is set to obtain directory information from another a directory service, or the directory setup can be deferred until first login.

- Some services are chosen and configured.

For a list of which services are enabled at startup, see the *Advanced Server Administration* guide.

Enabling the Firmware Password

After installing Snow Leopard Server, enable the Extensible Firmware Interface (EFI) password using the Firmware Password Utility. This prevents unauthorized users from starting up the server to install again or change settings.

For more information about the Firmware Password Utility, see Chapter 4, "Securing Global System Settings."

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

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

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

Protecting Hardware

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

The physical security of a server is an often overlooked aspect of computer security. Anyone with physical access to a computer (for example, to open the case, or plug in a keyboard, and so forth) has almost full control over the computer and the data on it.

For example, someone with physical access to a computer can:

- Restart the computer from another external disc, bypassing any existing login mechanism.
- Remove hard disks and use forensic data recovery techniques to retrieve data.
- Install hardware-based key-loggers on the local administration keyboard.

In your own organization and environment, you must decide which precautions are necessary, effective, and cost-effective to protect the value of your data and network.

For example, in an organization where floor-to-ceiling barriers might be needed to protect a server room, securing the air ducts leading to the room might also need to be considered. Other organizations might only need a locked server rack or an firmware password.

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

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

If you can't guarantee the physical security of the hard disk, consider using FileVault for each home folder. FileVault encrypts home folder content and guards against the content being compromised. For more information, see "Encrypting Home Folders" on page 151.

FileVault does not protect against the threat of an attacker tampering with files on the disk and reinstalling the drive. For example, an attacker could install a modified kernel, and use it to obtain your FileVault password by logging your keyboard keystrokes.

To prevent such an attack, lock your computer when it is unattended. Also, if you share your computer with others, limit those who have sudoer permissions. For information about limiting sudoers, see "Securing Directory Accounts" on page 319.

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

Preventing Wireless Eavesdropping

If you have installed Snow Leopard Server on a computer with wireless network access (for example, it has an Airport card or other wi-fi card installed), consider disabling wireless access to prevent eavesdropping.

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

Wireless access points that have access to your server should require encryption of the connection, user authentication (through the use of certificates or smart cards), and time-outs for connections.

If you need to use Wi-Fi, see *Snow Leopard Security Configuration* for information about how to leverage 802.1X for securing your Wi-Fi traffic.

Understanding Wireless Security Challenges

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

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

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

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

About OS Components

Special hardware, such as wireless networking cards and audio/video components, need driver software that runs at the kernel level. This driver software is implemented as kernel extensions ("kexts") in Mac OS X and are also known as OS components.

These kernel extensions can be removed from Mac OS X to prevent the use of a piece of hardware.

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

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

Removing Wi-Fi Support Software

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

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

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

To remove kernel extensions for Airport hardware:

1 Open the /System/Library/Extensions folder.

2 Drag the following file to the Trash:

IO80211Family.kext

3 Open Terminal and enter the following command:

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

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

4 Choose Finder > Secure Empty Trash to delete the files.

5 Restart the system.

From the command line:

```
# -----
# Protecting System Hardware
# -----
# Securing Wi-Fi Hardware
# -----
# Remove AppleAirport kernel extensions.
sudo rm -r /System/Library/Extensions/IO80211Family.kext

# Remove Extensions cache files.
sudo touch /System/Library/Extensions
```

Removing Bluetooth Support Software

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

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

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

To remove kernel extensions for Bluetooth hardware:

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

IOBluetoothFamily.kext

IOBluetoothHIDDriver.kext

- 3 Open Terminal and enter the following command:

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

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

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

From the command line:

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

# Suggested Setting.
# Remove Bluetooth kernel extensions.

# Remove Bluetooth kernel extensions.
sudo rm -r /System/Library/Extensions/IOBluetoothFamily.kext
sudo rm -r /System/Library/Extensions/IOBluetoothHIDDriver.kext

# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings.
# None
```

Removing IR Support Software

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

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

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

To remove kernel extensions for IR hardware support:

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

2 Drag the following file to the Trash:

AppleIRController.kext

3 Open Terminal and enter the following command:

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

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

4 Choose Finder > Secure Empty Trash to delete the file.

5 Restart the system.

From the Command Line:

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

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

# Available Settings.
# None
```

Preventing Unauthorized Recording

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

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

Removing Audio Support Software

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

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

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

To remove kernel extensions for audio hardware:

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

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

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

From the command line:

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

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

# Available Settings.
# None
```

Removing Video Recording Support Software

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

Note: The support for external iSight cameras should be removed on all machines. Removing only support for internal iSight cameras still leaves support for external cameras.

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

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

To remove kernel extensions for video hardware:

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

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

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

From the command line:

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

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

# Available Settings.
# None
```

Preventing Data Port Access

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

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

Also, by setting a firmware password using the Firmware Password Utility, you can prevent a physical Direct Memory Access (DMA) attack over FireWire. When the firmware password is set, any external device is denied direct access to computer memory content. For more information about the Firmware Password Utility, see “Using the Firmware Password Utility” on page 64.

Removing USB Support Software

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

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

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

To remove kernel extensions for specific hardware:

- 1 Open the /System/Library/Extensions folder.
- 2 To remove support for USB mass storage devices, drag the following file to the Trash:
IOUSBMassStorageClass.kext
- 3 Open Terminal and enter the following command:
`sudo touch /System/Library/Extensions`
The `touch` command changes the modified date of the /System/Library/Extensions folder. When the folder has a new modified date, the Extension cache files (located in /System/Library/) are deleted and rebuilt by Snow Leopard Server.
- 4 Choose Finder > Secure Empty Trash to delete the file.
- 5 Restart the system.

From the command line:

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

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

# Available Settings.
# None
```

Removing FireWire Support Software

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

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

To remove kernel extensions for specific hardware:

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

IOFireWireSerialBusProtocolTransport.kext

- 3 Open Terminal and enter the following command:

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

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

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

From the command line:

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

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

# Available Settings.
# None
```

System Hardware Modifications

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

Although disabling hardware in this manner is not as secure as physically disabling hardware, it is more secure than disabling hardware through System Preferences.

This method of disabling hardware components might not be sufficient to meet an organization's security policy. Consult your organization's operational policy to determine if this method is adequate.

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

- Airport
- Bluetooth
- Microphone
- Camera
- IR Port

Important: Attempting to remove components will void your warranty.

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

Securing Global System Settings

4

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

After installing and setting up Snow Leopard Server, make sure you protect your hardware and secure global system settings.

Securing System Startup

When a computer starts up, it first starts Extensible Firmware Interface (EFI). EFI is the software link between the motherboard hardware and the software operating system. EFI determine which partition or disk to load Mac OS X from. It also determines whether the user can enter single-user mode.

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

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

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

To secure startup, perform one of the following tasks:

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

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

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

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

Using the Firmware Password Utility

The Snow Leopard Server installation disc includes Firmware Password Utility, which you can use to enable an EFI password.

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

To use the Firmware Password Utility:

- 1 Log in with an administrator account and open the Firmware Password Utility (located on the Mac OS X installation disc in /Applications/Utilities/).
- 2 Click New.
- 3 Select “Require password to start this computer from another source.” To disable the EFI password, deselect “Require password to start this computer from another source.” You won’t need to enter a password and verify it. Disabling the EFI password is only recommended for installing Mac OS X.
- 4 In the Password and Verify fields, enter a new EFI password and click OK.
- 5 Close the Firmware Password Utility.

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

Using Command-Line Tools for Secure Startup

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

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

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

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

```
sudo nvram security-mode=full
```

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

From the command line:

```
# Securing Global System Settings
# -----
# Configuring Firmware Settings
# -----
# Default Setting.
# security-mode is off

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

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

Configuring Access Warnings

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

Enabling Access Warnings for the Login Window

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

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



To create a login window access warning:

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

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

Replace `Warning Text` with your access warning text.

- 3 Log out to test your changes.

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

From the command line:

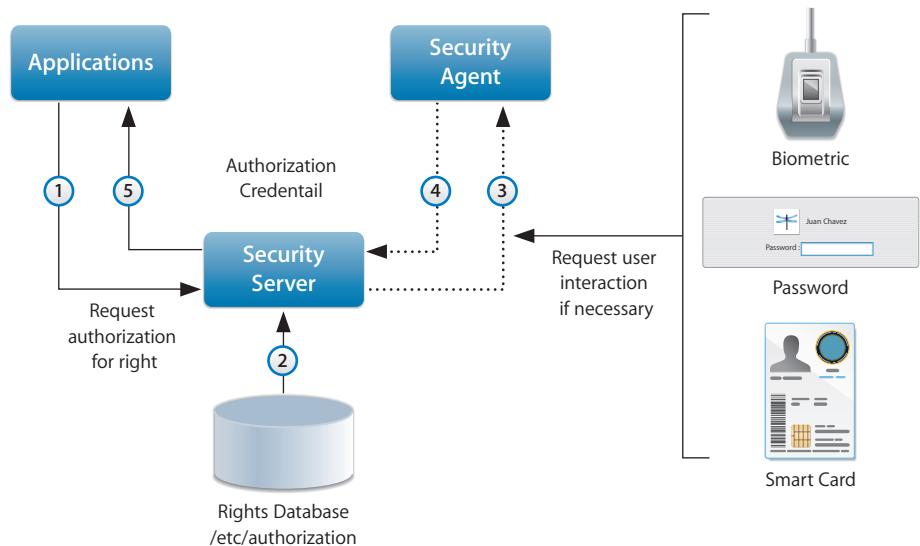
```
# Enabling Access Warning for the Login Window  
# -----  
# Create a login window access warning.  
sudo defaults write /Library/Preferences/com.apple.loginwindow  
    LoginwindowText "Warning Text"  
# You can also used the BannerSample project to create an access warning.
```

Understanding the AuthPlugin Architecture

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

For more information about /etc/authorization, see Chapter 29, “Managing Authorization Through Rights,” on page 363.

The following graphic shows the workflow of the Security Server.



When an application requests authorization rights from the security server the security server interrogates the rights database (/etc/authorization) to determine the mechanisms to be used for authentication.

If necessary, the security server requests user interaction through the security agent. The security agent then prompts the user to authenticate through the use of a password, smart card, or biometric reader.

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

The BannerSample Project

If your computer has developer tools installed, the sample code for the banner sample project is located in /Developer/examples/security/bannersample. You can modify and customize this sample banner code for your organization.

After you compile the code you can place it in the /Library/Security/SecurityAgentPlugins/ folder. Then modify the key `system.login.console` in the /etc/authorization file using Terminal.

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

To modify the /etc/authorization file:

- 1 Open Terminal.
- 2 Enter the following command:
`sudo pico /etc/authorization`
- 3 Locate the `system.login.console` key.
- 4 Add `<string>bannersample:test</string>` above `<string> builtin:smartcard-sniffer,privileged</string>`, as shown in bold below:

```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>comment</key>
<string>Login mechanism based rule. Not for general use, yet.</string>
<key>mechanisms</key>
<array>
<string>bannersample:test</string>
<string>builtin:smartcard-sniffer,privileged</string>
```

- 5 Save changes and exit the editor.
- 6 Restart the computer and verify that the banner appears.

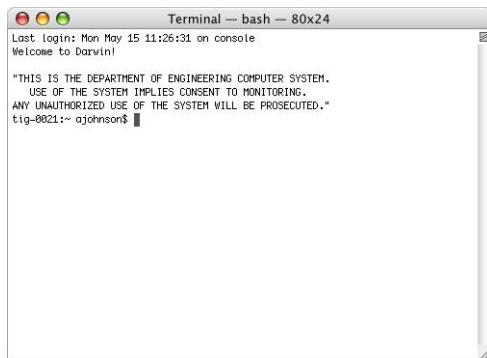
For additional information or support for the BannerSample project contact AppleFederal@apple.com.

Enabling Access Warnings for the Command Line

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

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

The following task must be performed by an administrator user using any text editor.



To create a command-line access warning:

- 1 Open Terminal.
- 2 Enter the following command to create the /etc/motd file:
`sudo touch /etc/motd`
- 3 Enter the following command to edit the /etc/motd file:
`sudo pico /etc/motd`
- 4 Enter your access warning message.
- 5 Save changes and exit the text editor.
- 6 Open a new Terminal window to test changes.

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

From the command line:

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

Turning On File Extensions

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

To turn file extensions on:

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

Securing Local Server Accounts

5

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

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

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

Types of User Accounts

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

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

The following table shows the access provided to user accounts.

User Account	User Access
Guest nonadministrator	Restricted user access (disabled by default)
Standard nonadministrator	Nonprivileged user access
Managed nonadministrator	Restricted user access
Delegated server administrator	Administer specified service configuration
Administrator	Full server configuration administration

User Account	User Access
Directory domain administrator	Administer the configured domains on the server
System administrator (root)	Unrestricted access to the server

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

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

Note: This chapter describes how to secure local accounts configured on Snow Leopard Server. For more information about securing user and group network accounts using Workgroup Manager, see Chapter 22, "Securing Network Accounts."

Guidelines for Creating Accounts

When you create user accounts, follow these guidelines:

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

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

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

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

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

Defining User IDs

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

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

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

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

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

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

User names never appear in the login window in Snow Leopard Server.

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

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

Securing the Guest Account

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

In security sensitive environments the guest account should remain disabled. If you enable the guest account, enable parental controls to limit what the user can do. Enabling parental control on an account does not defend against a determined attacker and should not be used as the primary security mechanism.

Whether or not the guest account is enabled, disable guest account access to shared files and folders by deselecting the “Allow guest to connect to shared folders” checkbox. If you permit the guest account to access shared folders, an attacker can easily attempt to access shared folders without a password.

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

Securing Nonadministrator Accounts

There are two types of nonadministrator user accounts: standard and managed.

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

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

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

Securing External Accounts

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

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

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

Protecting Data on External Volumes

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

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

Securing Directory-Based Accounts

A directory-based account is an account located on a directory server. A directory server contains user account records and important data for authenticating users.

If your computer is connected to a directory server, you can add directory users to your computer and grant them access. You can restrict a directory user account by using Parental Controls.

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

Avoiding Simultaneous Local Account Access

Monitoring user accounts and activities is important to securing your computer. This enables you to determine if an account is compromised or if a user is performing malicious tasks.

Avoiding Fast User Switching

Although the use of Fast User Switching is convenient when you have multiple local users on a single computer, avoid enabling it.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is using the computer.

Also, any external volumes attached to the computer are mounted when another user logs in, granting all users access to the volume and ignoring access permissions.

Avoiding Shared User Accounts

Avoid creating accounts that are shared by several users. Individual accounts maintain accountability. Each user should have his or her own standard or managed account.

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

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

Securing Administrator Accounts

Each administrator should have two accounts: a standard account for daily use and an administrator account for administrator access. Remember that the nonadministrative account should be used for most daily activity, especially when accessing the network or Internet.

The administrator's account should only be used when absolutely necessary to accomplish administrative tasks. To secure administrator accounts, restrict the distribution of administrator accounts and limit the use of these accounts.

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

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

About Tiered Administration Permissions

Mac OS X Server can use another level of access control for added security.

Administrators can be assigned to services they can configure. These limitations are enacted on a server-by-server basis. This method can be used by an administrator with no restrictions to assign administrative duties to other users.

In previous releases of Mac OS X Server, there were two classes of users: admin and everyone else. Admin users can make any change to the settings of any service or change any directory data including passwords and password policies.

In Snow Leopard Server, you can now grant individuals and groups specific administrative permissions without adding them to the UNIX "admin" group. In other words, you can make them service administrators.

There are two levels of permissions:

- **Administer:** This level of permission is analogous to being in the UNIX admin group. You can change any setting on the server for the designated server and service only.

- **Monitor:** This level of permission allows you to view Overview panes, Log panes, and other information panes in Server Admin, as well as general server status data in server status lists. You do not have access to saved service settings.

Any user or group can be given these permissions for all services or for selected services. The permissions are stored on a per-server basis.

The only users that can change the tiered administration access list are users that are in the UNIX admin group.

This results in a tiered administration model, where some administrators have more privileges than others for assigned services. This results in a method of access control for individual server features and services.

For example, Alice (the lead administrator) has control over all services on a given server and can limit the ability of other admin group users (like Bob and Cathy) to change settings on the server. She can assign DNS and Firewall service administration to Bob, while leaving mail service administration to Cathy.

In this scenario, Cathy can't change the firewall or any service other than mail. Likewise, Bob can't change any services outside of his assigned services.

Tiered administration controls are effective in Server Admin and the serveradmin command-line tool. They are not effective against modifying UNIX configuration files throughout the system. Protect UNIX configuration files with POSIX-type permissions or ACLs.

You can determine which services other admin group users can modify. To do this, the administrator making the determination must have full, unmodified access.

Server Admin updates to reflect what operations are possible for a user's permissions. For example, some services are hidden or the Settings pane is dimmed when you can only monitor that service.

Because the feature is enforced on the server side, the permissions also impact the usage of serveradmin, dscl, dsimport, and pwpolicy command-line tools because these tools are limited to the permissions configured for the administrator in use.

Defining Administrative Permissions

You can decide if a user or group can monitor or administer a server or service without giving them the full power of a UNIX administrative user. Assigning effective permissions to users creates a tiered administration, where some but not all administrative duties can be carried out by designated individuals.

To assign permissions:

- 1 Open Server Admin.
 - 2 Select a server, click the Settings button in the toolbar, and then click the Access tab.
 - 3 Click the Administrators tab.
 - 4 Select whether to define administrative permissions for all services on the server or for select services.
 - 5 If you define permissions by service, select the related checkbox for each service you want to turn on.
If you define permissions by service, be sure to assign administrators to all active services on the server.
 - 6 Click the Add (+) button to add a user or group from the users and group window.
To remove administrative permissions, select a user or group and click the Remove (-) button.
 - 7 For each user or group, select the permissions level next to the user or group name.
You can choose Monitor or Administer.
- The capabilities of Server Admin to administer the server are limited by this setting when the server is added to the Server list.

Avoiding Shared Administrator Accounts

Avoid creating accounts that are shared by several administrators. Individual accounts maintain accountability. Each user should have his or her own account.

System logs can track activities for each user account, but if several users share the same account, it becomes difficult to track which user performed an activity. For example, if several administrators share a single administrator account, it becomes harder to track which administrator performed a specific action.

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

Securing the Directory Domain Administrator Account

A directory domain can reside on a computer running Snow Leopard Server (for example, the LDAP folder of an Open Directory master, or other read/write directory domain) or it can reside on a non-Apple server (for example, a non-Apple LDAP or Active Directory server). Only a directory domain administrator can change the directory domain, including the managed accounts in the directory domain.

When configuring a directory domain administrator account, follow the same security guidelines as you would with any other administrator account.

Changing Special Authorizations for System Functions

You can modify the /etc/authorization configuration file to change authorizations for administrators and standard users.

WARNING: Changes to this file can have unanticipated negative results. Edit with caution.

To modify authorization by changing the /etc/authorization file:

- 1 Edit the /etc/authorization file using the pico tool, which allows for safe editing of the file.

The command must be run as root:

```
sudo pico /etc/authorization
```

- 2 When prompted, enter the administrator password.

This displays a property list for authorization, listing all available keys.

- 3 Locate the key you want to modify.

For example, to change who has access to unlock the screensaver, modify the system.login.screensaver key by changing the rule:

```
<key>rule</key>
  <string>authenticate-session-owner-or-admin</string>
```

to

```
<key>rule</key>
  <string>authenticate-session-owner</string>
```

Doing this restricts the administrator from unlocking the screensaver.

- 4 Save and quit pico.

Securing the System Administrator Account

The most powerful user account in Snow Leopard is the system administrator or root account. By default, the root account on Snow Leopard Server is enabled and uses the same password as the first created admin user. You should disable it using the following command:

```
dseableroot -d
```

Important: The system administrator or root account should only be used when absolutely necessary.

The most powerful user account in Mac OS X is the system administrator or root account. By default, the root account on Mac OS X is disabled and it is recommended you do not enable it.

The root account is primarily used for performing UNIX commands. Generally, actions that involve critical system files require you to perform those actions as root. However, using the `sudo` command, it is possible to perform root-level actions on an as-needed basis.

If you are logged in as a Snow Leopard Server administrator, you perform commands as root by using the `sudo` command. Snow Leopard Server logs actions performed using the `sudo` command. This helps you track misuse of the `sudo` command on a computer. Keep in mind that these logs can be edited if they are stored locally, so only grant sudo privileges to trusted users.

You can use the `su` command to log in to the command line as another user if you have that user's password. This includes the root user, if the root account is enabled. When you are logged in as root, you can use the `su` command to change users without a password.

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

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

If the root account is enabled, you can disable it by using an administrative account and the `dsonableroot` command. For example, the following command disables the root account.

```
sudo dsonableroot -d
```

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

Restricting sudo Usage

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

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

To restrict sudo usage by changing the `/etc/sudoers` file:

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

```
sudo visudo
```

- When prompted, enter the administrator password.

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

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

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

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

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

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

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

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

- Save and quit `visudo`.

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

Understanding Directory Domains

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

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

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

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

Users with mobile accounts have local and network home folders that combine to form portable home directories. When users save files, the files are stored in a local home folder. The portable home directory is a synchronized subset of a user's local and network home folders. For information about protecting your home folder, see Chapter 8, "Securing Data and Using Encryption."

Understanding Network Services, Authentication, and Contacts

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

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

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

Snow Leopard Server doesn't access disabled directory services, except for the local directory domain, which is always accessed. In addition to enabling and disabling services, you can use Directory Utility to choose the directory domains you want to authenticate with.

Directory Utility defines the authentication search policy that Snow Leopard uses to locate and retrieve user authentication information and other administrative data from directory domains.

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

Directory Utility also defines the contacts search policy that Snow Leopard 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, Snow Leopard Server searches each listed directory domain in turn until it finds the information it needs or reaches the end of the list without finding the information.

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

Configuring LDAPv3 Access

Snow Leopard Server 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.

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

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

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

Configuring Active Directory Access

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

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

Mutual authentication occurs when you bind to Active Directory servers.

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

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

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

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

Using Strong Authentication

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

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

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

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

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

Using Password Assistant to Generate or Analyze Passwords

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

You can choose from the following types of passwords:

- **Manual:** You enter a password and then Password Assistant gives you the quality level of your password. If the quality level is low, Password Assistant gives tips for increasing the quality level.
- **Memorable:** According to your password length requirements, Password Assistant generates a list of memorable passwords in the Suggestion menu.
- **Letters & Numbers:** According to your password length requirements, Password Assistant generates a list of passwords with a combination of letters and numbers.
- **Numbers Only:** According to your password length requirements, Password Assistant generates a list of passwords containing only numbers.

- **Random:** According to your password length requirements, Password Assistant generates a list of passwords containing random characters.
- **FIPS-181 compliant:** According to your password length requirements, Password Assistant generates a password that is FIPS-181 compliant (which includes mixed upper and lowercase, punctuation, and numbers).

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

Using Kerberos

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

Note: Snow Leopard Server supports Kerberos v5 but does not support Kerberos v4.

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

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

For example, consider two computers running Snow Leopard Server named "Mac01" and "Mac02." Mac02 has screen sharing and file sharing turned on. If Mac01 connects to a shared folder on Mac02, Mac01 can subsequently connect to screen sharing on Mac02 without supplying login credentials again.

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

Normally, after your computer obtains a Kerberos ticket in this manner, keep that Kerberos ticket until it expires. However, if you want to manually remove your Kerberos ticket, you can do so using the Kerberos utility in Snow Leopard Server.

To manually remove a Kerberos ticket:

- 1 Open Keychain Access (in /Applications/Utilities).
- 2 From the Keychain Access menu, choose Ticket Viewer.
- 3 In the Kerberos application's Ticket Cache window, find the key that looks like this:
`yourusername@LKDC:SHA1...`

It is followed by a long string of alphanumeric characters.

- 4 Click “Destroy Ticket” to delete that key.

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

Using Smart Cards

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

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

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

Smart card support is integrated into Snow Leopard Server and can be configured to work with the following services:

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

Using Tokens

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

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

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

Using Biometrics

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

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

The use of biometrics can enhance authentication by using something that is a part of you (such as your fingerprint).

Setting Global Password Policies

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

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

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

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

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

```
sudo pwpolicy -n /Local/Default -setglobalpolicy "minChars=12  
maxFailedLoginAttempts=3"
```

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

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

You can use `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 in Keychains

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

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

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

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

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

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

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

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

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

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

Note: You can use the `security` and `systemkeychain` commands to administer keychains, manipulate keys and certificates, and do just about anything the Security framework can do. For more information about this command, see its man page.

Using the Default User Keychain

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

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

To secure the login keychain:

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

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

To help you create a more secure password, use Password Assistant. For information, see "Using Password Assistant to Generate or Analyze Passwords" on page 84.

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

For information, see "Securing Keychains and Their Items" on page 91.

Creating Additional Keychains

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

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

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

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

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

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

To create a keychain and customize its authentication settings:

- 1 In Keychain Access, choose File > New Keychain.
- 2 Enter a name, select a location for the keychain, and click Create.
- 3 Enter a password, verify it, and click OK.
- 4 If you do not see a list of keychains, click Show Keychains.
- 5 Select the new keychain.
- 6 Choose Edit > Change Settings for keychain "*keychain_name*," and authenticate, if requested.
- 7 Change the "Lock after # minutes of inactivity" setting based on the access frequency of the security credentials included in the keychain.

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

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

If the security credentials are accessed infrequently, select "Lock after # minutes of inactivity" and specify a value, such as 1.

- 8 Select "Lock when sleeping."
- 9 Drag the security credentials from other keychains to the new keychain and authenticate, if requested.

You should have keychains that only contain related certificates. For example, you can have a mail keychain that only contains mail items.

- 10 If you are asked to confirm access to the keychain, enter the keychain password and click Allow Once.

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

Securing Keychains and Their Items

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

To secure a keychain item:

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

After you enable this option, Snow Leopard Server prompts you before giving a security credential to an application.

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

- 5 Select “Ask for Keychain password.”

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

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

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

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

Using Smart Cards as Keychains

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

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

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

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

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

Using Portable and Network Keychains

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

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

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

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

You can further protect portable keychains by storing them on biometric USB flash memory drives, or by storing portable drive contents in an encrypted file. For information, see "Encrypting Portable Files" on page 155.

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

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

- 1 Open Keychain Access.
- 2 If you do not see a list of keychains, click Show Keychains.
- 3 Choose Edit > Keychain List.
- 4 Note the location of the keychain you want to set up.
The default location is `~/Library/Keychains/`.
- 5 Click Cancel.
- 6 Select the keychain you want set up.
- 7 Choose File > Delete Keychain "`keychain_name`".

- 8** Click Delete References.
- 9** Copy the keychain files from the previously noted location to the portable drive.
- 10** Move the keychain to the Trash and use Secure Empty Trash to securely erase the keychain file stored on the computer.
For information, see “Using Secure Empty Trash” on page 160.
- 11** Open Finder and double-click the keychain file on your portable drive to add it to your keychain search list.

Use this chapter to set Snow Leopard Server system preferences to enhance system security and further protect against attacks.

System Preferences has many configurable preferences that you can use to customize system security. You can also manage these preferences using Workgroup Manager.

System Preferences Overview

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

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

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



If you log in as a user with administrator privileges, these preferences are unlocked unless you select "Require password to unlock each System Preferences pane" in Security preferences. For more information, see "Securing Security Preferences" on page 122.

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

Preferences that require authentication include the following:

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

This chapter lists each set of preferences included with Snow Leopard Server and describes modifications recommended to improve security.

Securing MobileMe Preferences

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

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

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

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



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



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



To disable MobileMe preferences:

- 1 Open MobileMe preferences.
- 2 Deselect “Synchronize with MobileMe.”
- 3 Make sure there are no computers registered for synchronization in the Advanced settings of the Sync pane.
- 4 Make sure iDisk Syncing is disabled in the iDisk pane.

From the command line:

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

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

# Available Settings.
# None
```

Securing Accounts Preferences

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



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

Note: If you are an administrator, password policies are not enforced when you change your password or when you change another user's password. Therefore, when you are changing passwords as an administrator, make sure you follow the password policy you set. For more information about password policies, see "Setting Global Password Policies" on page 87.

The password change dialog and the reset dialog (shown below) provide access to Password Assistant, an application that can analyze the strength of your password and assist you in creating a more secure password. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 84.



Consider the following login guidelines:

- Disable automatic login if enabled.
- Require that the user enter a name and a password, and that the user authenticate without the use of a password hint.
- Disable Restart, Sleep, and Shut Down buttons—the user cannot restart the computer without pressing the power key or logging in.
- Disable fast user switching if enabled—it is a security risk because it allows multiple users to be simultaneously logged in to a computer.

Although the use of Fast User Switching is convenient when you have multiple users on a single computer, there are cases in which you may not want to enable it.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is using the computer.

Also, some external volumes attached to the computer are mounted when another user logs in, granting all users access to the volume and ignoring access permissions.

Avoid creating accounts that are shared by several users. Individual accounts maintain accountability. Each user should have his or her own standard or managed account.

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

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

To securely configure Accounts preferences:

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

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

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

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

A screen similar to the following appears:



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

From the command line:

```
# Securing Accounts Preferences
# -----
# Change an account's password on a client system.
# Don't use this command if other users are also logged in.
sudo dscl /LDAPv3/127.0.0.1 passwd /Users/$User_name $Oldpass $Newpass

# Change an account's password on a server.
# Don't use this command if other users are also logged in.
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass

# Make sure there is no password hint set.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    RetriesUntilHint -int 0

# Disable Show the Restart, Sleep, and ShutDown Buttons.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    PowerOffDisable -bool yes

# Disable fast user switching. This command does not prevent multiple users
# from being logged in.
sudo defaults write /Library/Preferences/.GlobalPreferences
    MultipleSessionEnabled -bool NO
# Disable Automatic login.
sudo defaults write /Library/Preferences/.GlobalPreferences\
    com.apple.userspref.DisableAutoLogin -bool yes
```

Securing Appearance Preferences

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

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

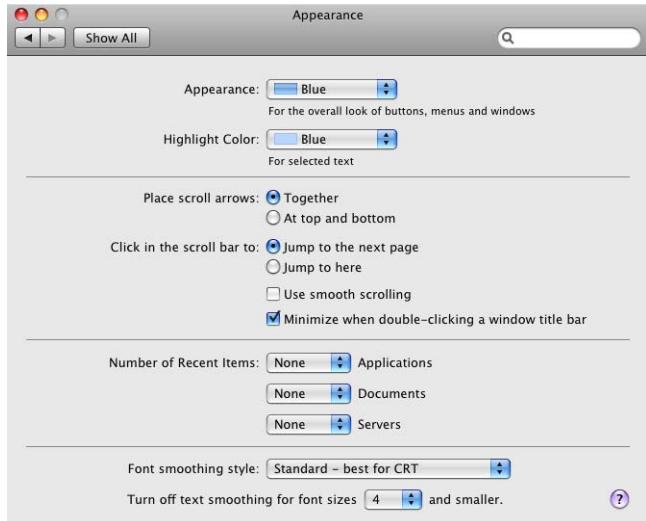
If intruders gain access to your computer, they can use recent items to quickly view your most recently accessed files. Additionally, intruders can use recent items to access authentication mechanisms for servers if the corresponding keychains are unlocked.

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

To securely configure Appearance preferences:

- 1 Open Appearance preferences.

A screen similar to the following appears:



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

From the command line:

```
# Securing Appearance Preferences
# -----
# Default Setting.
# MaxAmount 10

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

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

Securing Bluetooth Preferences

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

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

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

This does not prevent users from reenabling Bluetooth. You can restrict a user account's privileges so the user cannot reenable Bluetooth, but to do this, you remove several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 71.

Note: To remove Bluetooth support for peripherals, see "Removing Bluetooth Support Software" on page 55.

To securely configure Bluetooth preferences:

- 1 Open Bluetooth preferences.

A screen similar to the following appears:



- 2 Deselect "On."

From the command line:

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

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

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

Securing CDs & DVDs Preferences

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

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

This does not prevent users from reenabling automatic actions. To prevent the user from reenabling automatic actions, you must restrict the user's account so the user cannot open System Preferences. For more information on restricting accounts, see "Securing Nonadministrator Accounts" on page 74.

To securely configure CDs & DVDs preferences:

- 1 Open CDs & DVDs preferences.

A screen similar to the following appears:



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

From the command line:

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

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

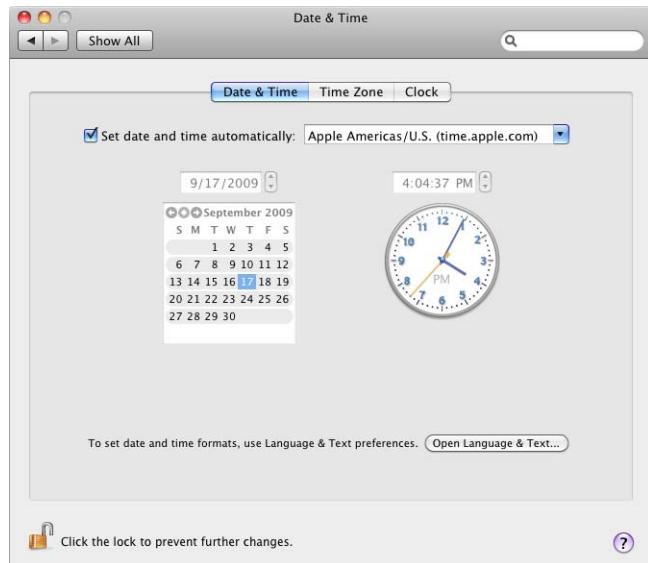
# Available Settings.
# action 1 = "Ignore"
# action 2 = "Ask what to do"
# action 5 = "Open other application"
# action 6 = "Run script"
# action 100 = "Open Finder"
# action 101 = "Open itunes"
# action 102 = "Open Disk Utility"
# action 105 = "Open DVD Player"
# action 106 = "Open iDVD"
# action 107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

Securing Date & Time Preferences

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

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

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



To securely configure Date & Time preferences:

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

A screen similar to the following appears:



4 Choose a time zone.

From the command line:

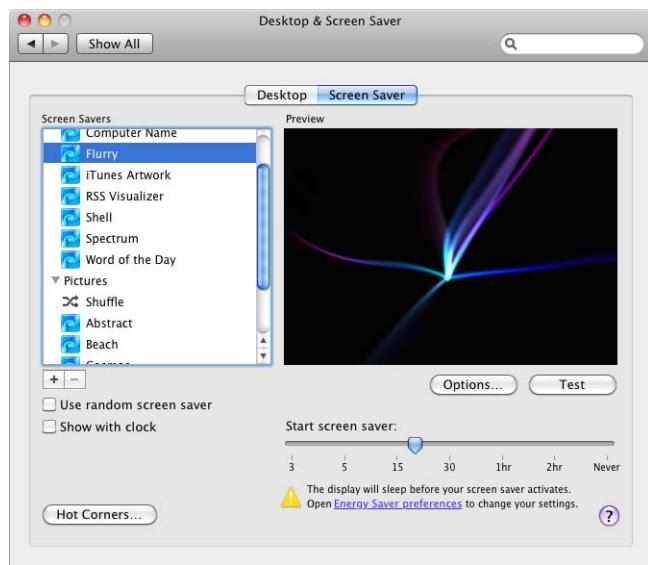
```
# Securing Date & Time Preferences
#
# Default Setting.
# NTP Server: time.apple.com
# Time Zone: Set time zone automatically using current location

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

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

Securing Desktop & Screen Saver Preferences

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

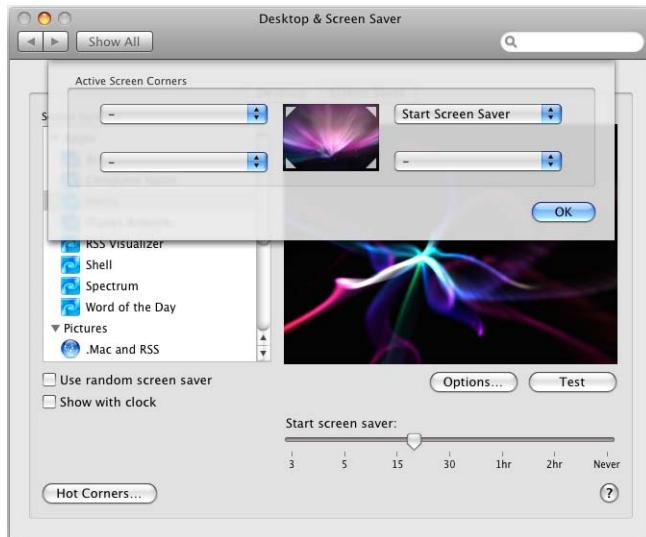


You can use several authentication methods to unlock the screen saver, including digital tokens, smart cards, and biometric readers.

You should also set a short inactivity interval to decrease the amount of time the unattended computer is unlocked. For information about requiring authentication for screen savers, see "Securing Security Preferences" on page 122.

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

By default, any admin can unlock any user's display.



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

This doesn't prevent users from reconfiguring their preferences. You can restrict a user's account privileges so the user cannot reconfigure preferences. Doing this removes several important user abilities, like the user's ability to change his or her password. For more information, see "Types of User Accounts" on page 71.

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, but don't set a screen corner to Disable Screen Saver.

From the command line:

```
# Securing Desktop & Screen Saver Preferences
#
# -----
# Default Setting.
# None

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

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

Securing Display Preferences

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

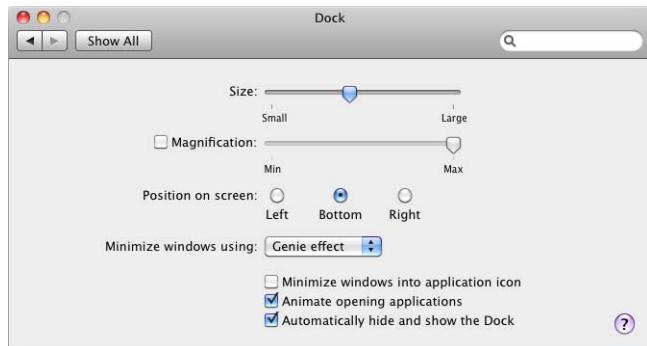
Securing Dock Preferences

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

To securely configure Dock preferences:

- 1 Open Dock preferences.

The following screen appears:



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

From the command line:

```
# Securing Dock Preferences
# -----
# Default Setting.
# None

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

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

Securing Energy Saver Preferences

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

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

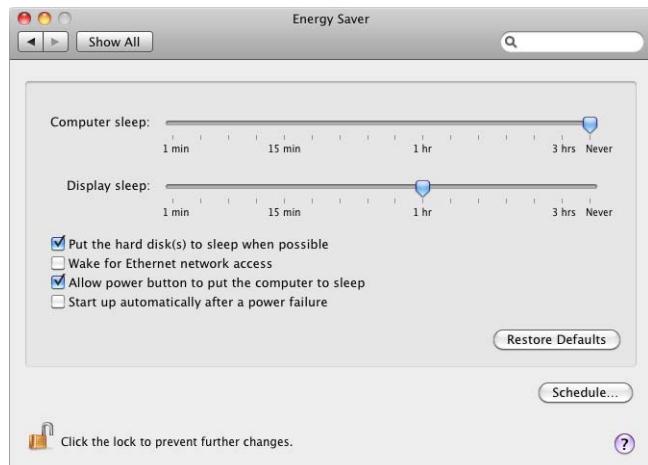
You can require authentication by use of a password, digital token, smart card, or biometric reader to reactivate the computer (see "Securing Security Preferences" on page 122). This is similar to using a password-protected screen saver.

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

To securely configure Energy Saver preferences:

- 1 Open Energy Saver preferences.

A screen similar to the following appears:



- 2 From the Sleep pane, set "Put the computer to sleep when it is inactive for" to Never.
- 3 Select "Put the hard disk(s) to sleep when possible" and then click the "Options" pane.
- 4 Deselect "Wake for Ethernet network access" and "Start up automatically after a power failure."

From the command line:

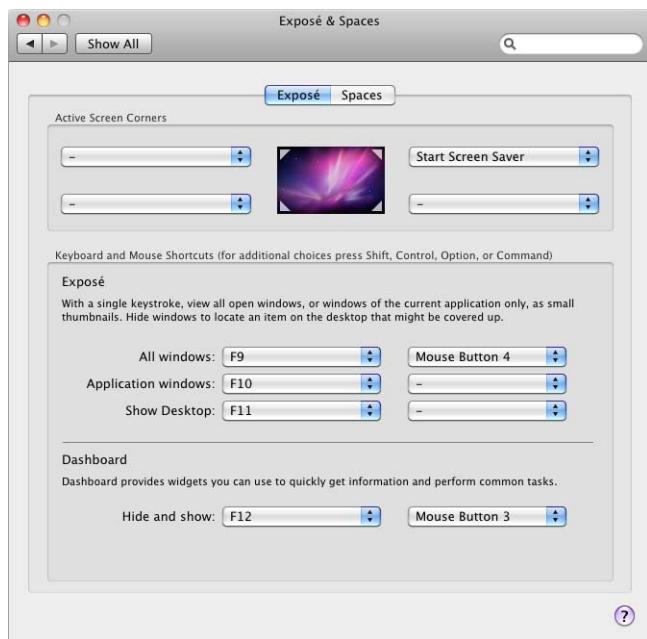
```
# Securing Energy Saver Preferences
# -----
# Default Setting.
# None

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

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

Securing Exposé & Spaces Preferences

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



For information about requiring authentication for the screen saver, see “Securing Security Preferences” on page 122.

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

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

This doesn't prevent users from reconfiguring their preferences. You can restrict a user account's privileges so the user cannot reconfigure preferences. To do this, you remove several important user abilities, like the user's ability to change his or her password. For more information, see “Types of User Accounts” on page 71.

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

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

From the command line:

```
# Securing Exposé & Spaces Preferences  
# -----  
# Default Setting.  
# Enabled  
  
# Suggested Setting.  
# Disable dashboard.  
sudo launchctl unload -w /System/Library/LaunchDaemons/  
    com.apple.dashboard.advisory.fetch.plist  
  
# Available Settings.  
# Enabled or Disabled
```

Securing Language & Text Preferences

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

Securing Keyboard Preferences

If you are not using a Bluetooth keyboard, turn Bluetooth off. If you are using a Bluetooth keyboard, disable allowing Bluetooth devices to awake the computer in the advanced section of Bluetooth preferences. For more information about Bluetooth, see “Securing Bluetooth Settings” on page 117.

Securing Mouse Preferences

If you are not using a Bluetooth mouse, turn Bluetooth off. If you are using a Bluetooth mouse, disable allowing Bluetooth devices to awake the computer in the advanced section of Bluetooth preferences. For more information about Bluetooth, see “Securing Bluetooth Preferences” on page 103.

Securing Bluetooth Settings

If you have a Bluetooth module installed in your computer or if you are using an external USB Bluetooth module, you can set up your computer to use Bluetooth to send and receive files with other Bluetooth-enabled computers or devices.

You can control how your computer handles files that are exchanged between Bluetooth devices. You can choose to accept or refuse files sent to your computer and choose which folder other devices can browse.

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

Restricting Access to Specified Users

If you are in an environment where you would like to share files with another computer or device, use the Bluetooth Sharing options and Bluetooth preferences to securely enable Bluetooth and avoid unauthorized access to your computer.

Bluetooth options should always require pairing and be set to "Ask What to Do" when receiving or sharing items.

When configuring Bluetooth preferences, to secure Bluetooth sharing, use the Discoverable option only while you are setting up the Bluetooth computer or device. After the device is configured, disable the Discoverable option to prevent unauthorized users from discovering your Bluetooth connection.

In the advanced section of Bluetooth preferences, make sure that "Allow Bluetooth devices to wake this computer" and "Share my internet connection with other Bluetooth devices" are not selected.

From the command line:

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

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

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

Securing Network Preferences

To secure Network preferences, disable unused hardware devices listed in Network preferences and IPv6. You should also use a static IP address when possible. A DHCP IP address should be used only if necessary.

Disabling Unused Hardware Devices

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



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

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

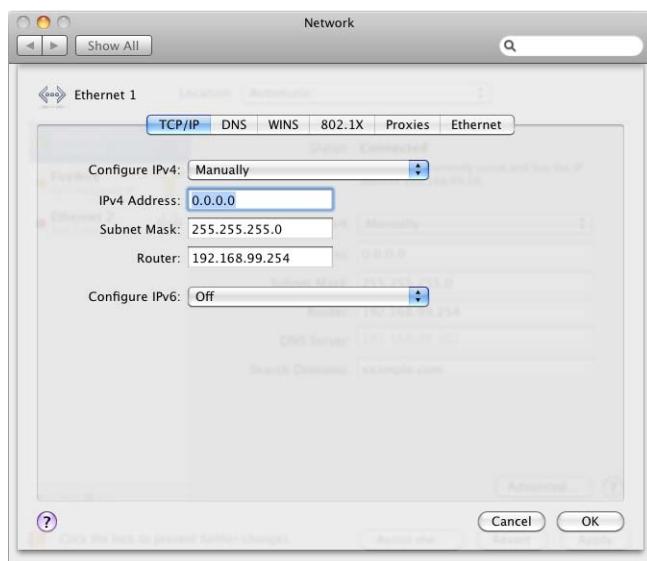
An address size of 128 bits is large enough to support a large number of addresses. This allows more addresses or nodes than are otherwise available. IPv6 also provides more ways to set up the address and simplifies autoconfiguration.

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

To securely configure Network preferences:

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

A screen similar to the following appears:



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

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

- 9 Click OK.

From the command line:

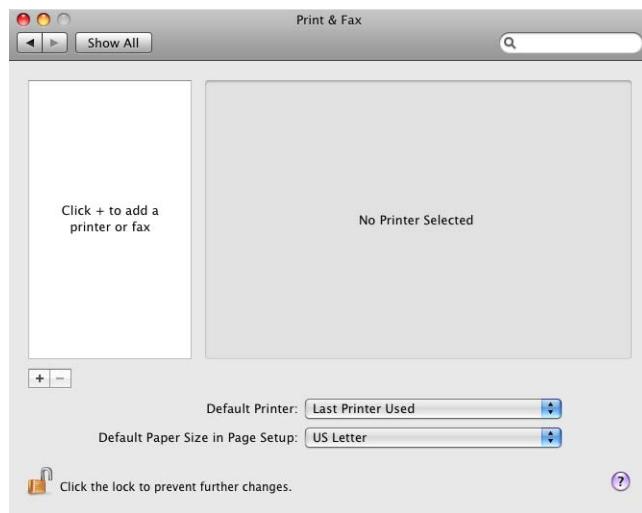
```
# Securing Network Preferences
# -----
# Default Setting.
# Enabled

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

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

Securing Print & Fax Preferences

The Print & Fax preferences screen looks like this:



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

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

Your printer can be accessed using the CUPS web interface (<http://localhost:631>). By default:

- The CUPS web interface cannot be accessed remotely. It can only be accessed by the local host.
- The titles of all print jobs are available to all users of the system.
- The titles of all print jobs are available to everyone with access to the CUPS web interface.

CUPS also offers the ability to browse the network for available printers. Manually specifying available printers is more secure. You can create policies in CUPS that restrict users from such actions as canceling jobs or deleting printers using the CUPS web interface. For more information about creating CUPS policies, see:

<http://localhost:631/help/policies.html>

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

To securely configure Print & Fax preferences:

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

A screen similar to the following appears:



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

From the command line:

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

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

# Available Settings.
# Enabled or Disabled
```

Securing Security Preferences

The settings in Security preferences cover a range of Snow Leopard Server security features, including login options, FileVault, and firewall protection.

General Security

Consider the following general security guidelines:

- **Wake computer:** Require a password to wake this computer from sleep or screen saver. This helps prevent unauthorized access on unattended computers. Although there is a lock button for Security preferences, users don't need to be authorized as an administrator to make changes. Enable this password requirement for every user account on the computer.
- **Automatic login:** Disabling automatic login is necessary for any level of security. If you enable automatic login, an intruder can log in without authenticating. Even if you automatically log in with a restricted user account, it is still easier to perform malicious actions on the computer.
- **Location Services:** Disabling location services prevents information about the location of your computer from being provided to applications.

- **Infrared receiver:** If you are not using a remote control, disable the infrared receiver. This prevents unauthorized users from controlling your computer through the infrared receiver. If you use an Apple IR Remote Control, pair it to your computer by clicking Pair. When you pair it, no other IR remote can control your computer.

FileVault Security

Mac OS X includes FileVault, which encrypts information in your home folder.

FileVault uses the government-approved 128-bit (AES-128) encryption standard keys, and supports the Advanced Encryption Standard with 256-bit (AES-256) keys. For more information about data encryption, see Chapter 8, “Securing Data and Using Encryption.”

For more information about FileVault, see “Encrypting Home Folders” on page 151.



To securely configure Security preferences:

- 1 Open Security preferences.
- 2 In the General pane, select the following:
 - “Require password immediately after sleep or screen saver begins”
- 3 Select the “Disable Location Services” checkbox, if available.
- 4 Select the “Disable remote control infrared receiver” checkbox.
- 5 In the FileVault pane, click “Turn on FileVault.”
- 6 Enter a password in the Master Password and verify fields.
- 7 Authenticate with your account password.
- 8 Select “Use secure erase” and click “Turn on FileVault.”
- 9 Restart the computer.

From the command line:

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

# Suggested Setting.
# Enable Require password to wake this computer from sleep or screen saver.
sudo defaults -currentHost write com.apple.screensaver askForPassword -int
    1
# Disable IR remote control.
sudo defaults write /Library/Preferences/com.apple.driver.AppleIRController
    DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
sudo /System/Library/CoreServices/ManagedClient.app/Contents/Resources/\
createmarketaccount
# Enable Firewall.
# Replace value with
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
sudo defaults write /Library/Preferences/com.apple.alf globalstate -int
    value
```

Securing Sharing Preferences

By default, every service listed in Sharing preferences is disabled except for remote login (SSH). Do not enable these services unless you use them. The following services are described in detail in *Snow Leopard Security Configuration*.

Service	Description
DVD or CD Sharing	Allows users of other computers to remotely use the DVD or CD drive on your computer.
Screen Sharing	Allows users of other computers to remotely view and control the computer.
Scanner Sharing	Allows other computers to access a scanner connected to this computer.
Remote Login	Allows users to access the computer remotely by using SSH. If you require the ability to perform remote login, SSH is more secure than telnet, which is disabled by default.
Remote Management	Allows the computer to be accessed using Apple Remote Desktop.
Remote Apple Events	Allows the computer to receive Apple events from other computers.
Bluetooth Sharing	Allows other Bluetooth-enabled computers and devices to share files with your computer.

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

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

For more information about these services and the firewall and sharing capabilities of Snow Leopard, see *Snow Leopard Security Configuration*.

To securely configure Sharing preferences:

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

From the command line:

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

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

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

Securing Software Update Preferences

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

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



You can install and verify updates on a test computer before installing them on your operational computer. For more information about how to manually update your computer, see “Updating Manually from Installer Packages” on page 48.

After transferring installer packages to your computer, verify the authenticity of the installer packages. For more information, see “Verifying the Integrity of Software” on page 50.

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

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

To disable automated Software Updates:

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

From the command line:

```
# Securing Software Updates Preferences
# -----
# Default Setting.
# Check for Updates: Enabled
# Check Updates: Weekly

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

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

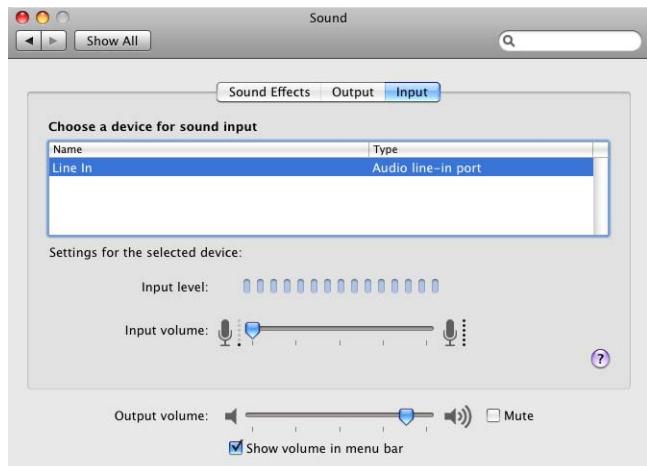
Securing Sound Preferences

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

To securely configure Sound preferences:

- 1 Open Sound preferences.

A screen similar to the following appears:



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

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

From the command line:

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

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

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

Securing Speech Preferences

Snow Leopard Server includes speech recognition and text-to-speech features, which are disabled by default.

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

The following shows the Speech preferences pane:



The following shows the Text to Speech pane:



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

To 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.

From the command line:

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

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

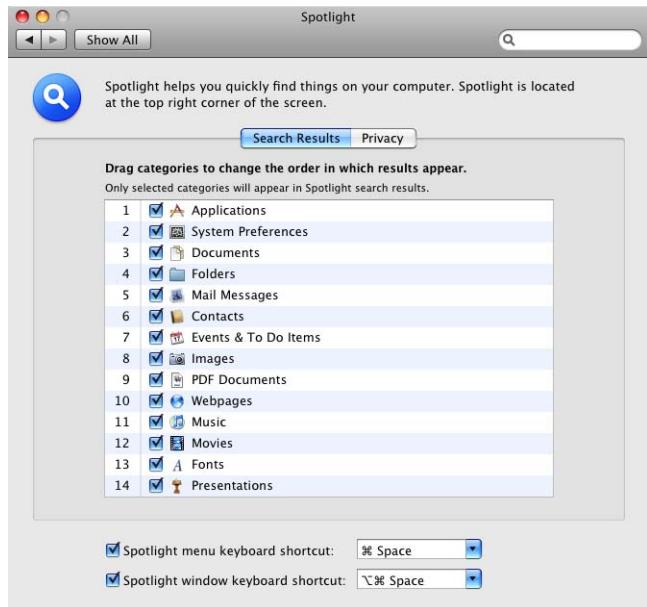
# Available Setting.
# Each item can be set to ON or OFF.
# OFF: -bool false
# ON: -bool true
```

Securing Spotlight Preferences

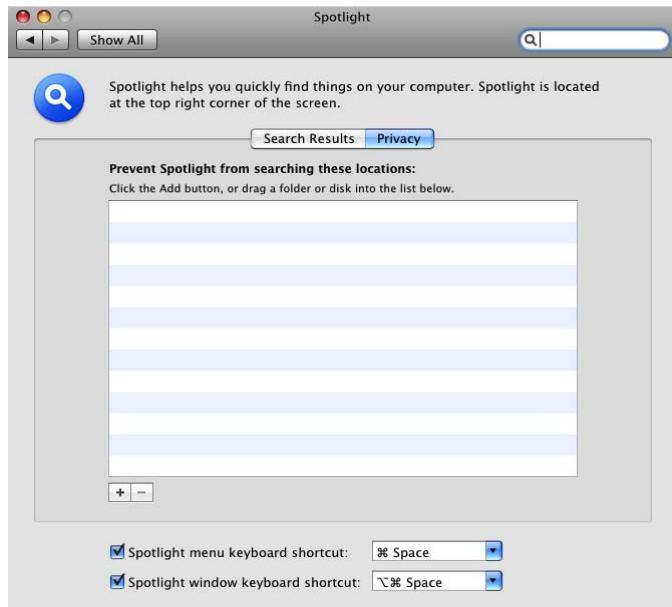
You can use Spotlight to search your computer for files. Spotlight searches the name and meta-information associated with each file and the contents of each file.

Spotlight finds files regardless of their placement in the file system. You must still properly set access permissions on folders containing confidential files. For more information about access permissions, see Chapter 8, “Securing Data and Using Encryption.”

The Spotlight Preferences Search Results pane appears:



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



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

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

To securely configure Spotlight preferences:

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

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

Note: To prevent users from reenabling Spotlight, remove the rights to access the .Spotlight-V100 folder at the root level of your drive (./.Spotlight-V100/).

From the command line:

```
# Securing Spotlight Preferences
# -----
# Default Setting.
# ON for all volumes

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

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

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

Securing Startup Disk Preferences

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



Be careful when selecting a startup volume:

- Choosing a network install image reinstalls your operating system and might erase the contents of your hard disk.
- If you choose a FireWire volume, your computer starts up from the FireWire disk plugged into the current FireWire port for that volume. If you connect a different FireWire disk to that FireWire port, your computer starts from the first valid Snow Leopard Server volume available to the computer (if you have not enabled the firmware password).
- When you enable a firmware password, the FireWire volume you select is the only volume that can start the computer. The computer firmware locks the FireWire Bridge Chip GUID as a startup volume instead of the hard disk's GUID (as is done with internal hard disks). If the disk inside the FireWire drive enclosure is replaced by a new disk, the computer can start from the new disk without using the firmware password. To avoid this intrusion make sure your hardware is physically secured. 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 52.

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

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

For more information about enabling a firmware password, see “Using the Firmware Password Utility” on page 64.

To select a startup disk:

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

From the command line:

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

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

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

Securing Time Machine Preferences

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

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

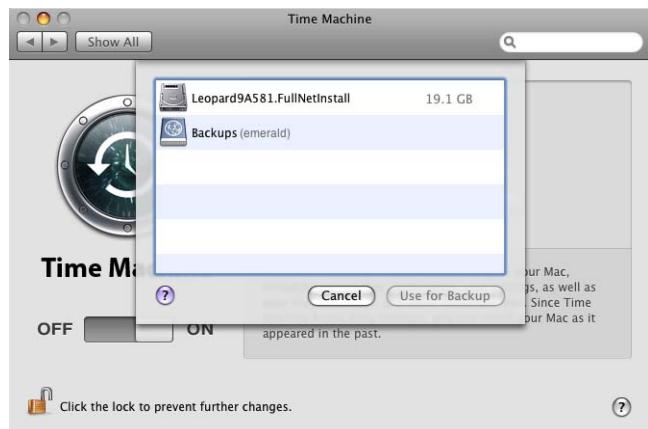
Information stored on your backup disk is not encrypted and can be read by other computers that are connected to your backup disk. Keep your backup disk in a physically secure location to prevent unauthorized access to your data.



To enable Time Machine:

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

A screen similar to the following appears:



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

From the command line:

```
# Securing Time Machine Preferences
# -----
# Default Setting.
# OFF

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

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

Securing Universal Access Preferences

Universal Access preferences are disabled by default. However, if you use an assistive device, follow these guidelines:

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

From the command line:

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

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

# Available Setting.
# None
```

Securing System Swap and Hibernation Storage

Use this chapter to protect data in swap files from being readable.

The data that an application writes to random-access memory (RAM) might contain sensitive information, such as user names and passwords. Mac OS X writes the contents of RAM to your local hard disk to free memory for other applications. The RAM contents stored on the hard disk are kept in a file called a swap file.

While the data is on the hard disk, it can be easily viewed or accessed if the computer is later compromised. You can protect this data by securing the system swap file in case of an attack or theft of your computer.

System Swap File Overview

When your computer is turned off, information stored in RAM is lost, but information stored by virtual memory in a swap file can remain on your hard drive in unencrypted form. The Mac OS X virtual memory system creates this swap file in order to reduce problems caused by limited memory.

The virtual memory system can swap data between your hard disk and RAM. It's possible that sensitive information in your computer's RAM will be written to your hard disk in the swap file while you are working, and remain there until overwritten. This data can be compromised if your computer is accessed by an unauthorized user, because the data is stored on the hard disk unencrypted.

When your computer goes into hibernation, it writes the content of RAM to the /var/vm/sleepimage file. The sleepimage file contains the contents of RAM unencrypted, similar to a swap file.

You can prevent your sensitive RAM information from being left unencrypted on your hard disk by enabling secure virtual memory to encrypt the swap file and the /var/vm/sleepimage file (where your hibernation files are stored).

Note: Using FileVault in combination with the “Secure Virtual Memory” feature provides protection from attacks on your sensitive data when it is stored on the hard disk.

Encrypting System Swap

You can prevent sensitive information from remaining on your hard disk and eliminate the security risk by using secure virtual memory. Secure virtual memory encrypts the data being written to disk.

You must restart the server for the change to take effect.

To turn on secure virtual memory from the command line:

```
#  
# Securing System Swap and Hibernation Storage  
# -----  
# Enable secure virtual memory.  
sudo defaults write /Library/Preferences/com.apple.virtualMemory \  
    UseEncryptedSwap -bool YES  
  
# Restart to take effect.  
# sudo shutdown -r now
```

Securing Data and Using Encryption

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

Your data is the most valuable part of your computer. By using encryption you can protect data in 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. In addition, by using the secure erase feature of Snow Leopard, deleted data is completely erased from the computer.

About Transport Encryption

Any data that is transferred to or from the server can be kept secure by either encrypting the transmission, the payload, or both.

Transferring data securely across a network involves encrypting the packet contents sent between computers. Mac OS X Server can provide Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) as the cryptographic protocols that provide secure communications on the Internet for such things as web browsing, mail, and other data transfers.

These encryption protocols allow client and server applications to communicate in a way that helps prevent eavesdropping, tampering, and message forgery.

TLS provides endpoint authentication and communications privacy over the Internet using cryptography. These encrypted connections authenticate the server (so its identity is ensured) but the client remains unauthenticated.

To have mutual authentication (where each side of the connection is assured of the identity of the other), use a public key infrastructure (PKI) for the connecting clients.

Mac OS X Server makes use of OpenSSL and has integrated transport encryption into the following tools and services:

- Server administration using Server Admin and Server Preferences
- User and group management using Workgroup Manager
- Address Book Server
- iCal Server
- iChat Server
- Mail Service
- Open Directory
- Podcast Producer
- RADIUS
- SSH
- VPN (L2TP)
- Web service

Each service requires transport encryption to be enabled individually. For more information on securing data transmission for a service, see the service's configuration details.

About Payload Encryption

Rather than encrypting the transfer of a file across the network, you can encrypt the contents of the file instead. Files with strong encryption might be captured in transit, but are still unreadable.

Most transport encryption requires the participation of both parties in the transaction.

Some services (such as SMTP mail service) can't reliably use such techniques, so encrypting the file itself is the only method of reliably securing the file content.

To learn more about encrypting your files, see "Encrypting Portable Files" on page 155.

About File and Folder Permissions

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

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

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

Setting POSIX Permissions

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

Viewing POSIX Permissions

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

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

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

To view folder or file permissions:

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

```
ls -l
```

Output similar to the following appears:

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

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

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

Interpreting POSIX Permissions

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

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

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

- The `d` of the POSIX permissions signifies that `newfolder` is a folder.
- The first three letters after the `d` (`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, users who can access `ajohnson's ~/Documents/` folder can open the `NewFolder` folder but can't modify or open the `file.txt` file. Read POSIX permissions are propagated through the folder hierarchy.

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

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

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

You might see a `t` for others' privileges on a folder used for collaboration. This `t` is sometimes known as the sticky bit. Enabling the sticky bit on a folder prevents people from overwriting, renaming, or otherwise modifying other people's files. This can be common if several people are granted `rx` access.

The sticky bit 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.

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

Modifying POSIX Permissions

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

To modify POSIX permissions:

- 1 In Terminal, enter the following to add write permission for the group to file.txt:

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

- 2 View the permissions using the `ls` command.

```
ls -l
```

- 3 Validate that the permissions are correct.

```
computer:~/Documents ajohnson$ ls -l  
total 12346  
drwxr-xr-x 2 ajohnson staff 68 Apr 28 2006 NewFolder  
-rw-rw-r-- 1 ajohnson staff 43008 Apr 14 2006 file.txt
```

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

Setting File and Folder Flags

You can also protect files and folders by using flags. These flags, or permission extensions, override standard POSIX permissions. They can only be set or unset by the file's owner or an administrator using `sudo`. Use flags to prevent the system administrator (root) from modifying or deleting files or folders.

To enable and disable flags, use the `chflags` command.

Viewing Flags

Before setting or changing file or folder flags, view the current flag settings.

To display flags set on a folder:

```
ls -lo secret  
-rw-r--- 1 ajohnson staff uchg 0 Mar 1 07:54 secret
```

This example displays the flag settings for a folder named `secret`.

Modifying Flags

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

To lock or unlock a folder using flags:

```
sudo chflags uchg folderName
```

In this example, the folder named secret is locked.

To unlock the folder, change `uchg` to `nouchg`:

```
sudo chflags nouchg secret
```

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

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

Setting ACL Permissions

For greater flexibility in configuring and managing file permissions, Snow Leopard Server implements ACLs. An ACL is an ordered list of rules called ACEs that control file permissions. Each ACE contains the following components:

- User—owner, group, and other
- Action—read, write, or execute
- Permission—allow or deny the action

The rules specify the permissions to be granted or denied to a group or user and controls how the permissions are propagated through a folder hierarchy.

ACLs in Snow Leopard Server let you set file and folder access permissions for multiple users and groups, in addition to standard POSIX permissions. This makes it easy to set up collaborative environments for file sharing and uninterrupted workflows without compromising security.

Snow Leopard Server 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, ACEs are considered in order. The first ACE that applies to a user and action determines the permission and no further ACEs are evaluated. If no ACEs apply, standard POSIX permissions determine access.

Enabling ACL Permissions

By default, ACLs are enabled in Snow Leopard Server. If they are turned off, you must enable the volume to support ACLs.

The following example uses the `fsaclctl` command to enable ACLs on a Snow Leopard Server startup volume:

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

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

Modifying ACL Permissions

You can set ACL permissions for files. The `chmod` command enables an administrator to grant read, write, and execute privileges to specific users for a single file.

To set ACL permissions for a file:

- 1 Allow specific users to access specific files.

For example, to allow Anne Johnson permission to read the file `secret.txt`, enter the following in Terminal:

```
chmod +a "ajohnson allow read" secret.txt
```

- 2 Allow specific groups of users to access specific files.

For example, to allow the engineers group permission to delete the file `secret.txt`, enter the following in Terminal:

```
chmod +a "engineers allow delete" secret.txt
```

- 3 Deny access privileges to specific files.

For example, to prevent Tom Clark from modifying the file `secret.txt`, enter the following in Terminal:

```
chmod +a "tclark deny write" secret.txt
```

- 4 View and validate the ACL modifications with the `ls` command:

```
ls -le secret.txt
-rw----- 1 ajohnson admin 43008 Apr 14 2006 secret.txt
0: ajohnson allow read
1: tclark deny write
2: engineers allow delete
```

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

Changing Global Umask for Stricter Default Permissions

Every file or folder has POSIX permissions associated with it. When you create a file or folder, the umask setting determines these POSIX permissions.

The umask value is subtracted from the maximum permissions value (777) to determine the default permission value of a newly created file or folder. For example, a umask of 022 results in a default permission of 755.

The default umask setting 022 (in octal) removes group and other write permissions. Group members and other users can read and run these files or folders. Changing the umask setting to 027 enables group members to read files and folders and prevents others from accessing the files and folders. If you want to be the only user to access your files and folders, set the umask setting to 077.

To change the globally defined umask setting, change the umask setting in /etc/launchd.conf.

You must be logged in as a user who can use `sudo` to perform these operations and you must use the decimal equivalent, not an octal number.

Note: Users and applications can override default umask settings at any time for their own files.

WARNING: Many installations depend on the default umask setting. There can be unintended and possibly severe consequences to changing it. Instead, use inherited permissions, which are applied by setting permissions on a folder. All files contained in that folder will inherit the permissions of that folder.

To change the global umask file permission:

- 1 Sign in as a user who can use `sudo`.
- 2 Open Terminal.
- 3 Change the umask setting:

```
sudo echo "umask 027" >> /etc/launchd.conf
```

This example sets the global umask setting to 027.

- 4 Log out.

Changes to umask settings take effect at the next login.

Users can use the Finder’s Get Info window or the `chmod` command-line tool to change permissions for files and folders.

Restricting Setuid Programs

When applied to a program, the POSIX setuid (set user ID) permission means that when the program runs, it will run at the privilege level of the file's owner. The POSIX setgid (set group ID) permission is analogous. To see an example of a file with the setuid bit, run the ls command on the ping program as follows:

```
ls -l /sbin/ping  
-r-sr-xr-x 1 root wheel 68448 Nov 28 2007 /sbin/ping
```

The setuid bit is represented with an "s" in the field of permissions, in the position that contains the file owner's execute permission. The program runs with the privilege level of the file's owner. The owner of the file is root, so when ping is executed—no matter who executes it—it runs as root. For setgid programs, an "s" appears in the group execute permission and the file runs with the privileges of the group owner.

The setuid bit is necessary for many programs on the system to perform the specific, privileged tasks for which they are designed for. The ping program, for example, is setuid because it must be able to engage in network communication that is only possible with root privileges.

To find setuid programs on the system, use the following command:

```
sudo find / -perm -04000 -ls
```

To find setgid programs, use -02000 instead of -04000.

Mac OS X includes approximately 75 setuid programs. Many of these programs need the setuid bit for normal system operation. However, other programs may need the setuid bit only if certain functionality is needed, or only if administrators need to use the program.

Because attackers try to influence or co-opt the execution of setuid programs to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

If a program is needed but has had its setuid bit stripped, an administrator can run the program using sudo, which runs the program as the root user. An administrator can also temporarily enable the setuid bit while the program is needed, and then disable it again afterward.

Stripping Setuid Bits

To strip the setuid or setgid bit from a program, use the following command:

```
sudo chmod -s programname
```

The following programs can have their setuid bit removed, unless needed for the purpose shown in the second column::

Application	Related Service
/System/Library/CoreServices/	Apple Remote Desktop
RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent	
/usr/bin/at	Job Scheduler
/usr/bin/atq	Job Scheduler
/usr/bin/atrm	Job Scheduler
/usr/bin/crontab	Job Scheduler
/usr/bin/postdrop	Postfix Mail
/System/Library/PrivateFrameworks/DesktopServicesPriv.framework/Versions/A/Resources/Locum	Performing Privileged File Operations using Finder
/usr/bin/postqueue	Postfix Mail Queue
/usr/bin/procmail	Mail Processor
/usr/bin/wall	User Messaging
/usr/bin/write	User Messaging
/usr/bin/chrfn	Change Finger Information
/System/Library/Printers/IOMs/LPRIOM.plugin/Contents/MacOS/LPRIOMHelper	Printing
/usr/sbin/traceroute	Trace Network Path
/usr/sbin/traceroute6	Trace Network Path
/sbin/mount_fs	Mounting NFS Filesystems
/usr/bin/ipcs	IPC Statistics
/bin/rpc	Remote Access (unsecure)
/usr/bin/rlogin	Remote Access (unsecure)
/usr/bin/rsh	Remote Access (unsecure)
/usr/lib/sa/sadc	System Activity Reporting
/usr/sbin/scselect	Allowing non-administrators to change Network Location

Important: The Repair Permissions feature of Disk Utility reenables the setuid bit on these programs. Software updates may also reenable the setuid bit on these programs. To achieve some persistence for the permissions change, create a shell script to strip the bits and then implement a launchd job (for the root account) to execute this script every half hour. This ensures that no more than half an hour passes from the time a system update is applied until the setuid bits are removed.

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

Using ACLs to Restrict Usage of Setuid Programs

You can also use the ACL feature of Mac OS X to restrict the execution of setuid programs.

Restricting the execution of setuid programs to administrators prevents other users from executing those programs. It should also prevent attackers who have ordinary user privileges from executing the setuid program and trying to elevate their privileges.

All users on the system are in the “staff” group, so the commands below allow members of the admin group to execute <program name> but deny that right to members of the staff group:

```
sudo chmod +a "group:staff deny execute" <program name>
sudo chmod +a# 0 "group:admin allow execute" <program name>
```

To view the ACL:

```
ls -le <program name>
```

The output looks something like this:

```
-r-sr-xr-x+ 1 root wheel 12345 Nov 28 2007 <program name>
0: group:admin allow execute
1: group:staff deny execute
```

Because the ACL is evaluated in order from top to bottom, users in the admin group are permitted to execute the program. The following rule denies that right to all users.

Important: Although the “Repair Permissions” feature of Disk Utility does not strip ACLs from programs, software updates might strip these ACLs. In order to achieve some persistence for the ACLs, create a shell script to set the ACLs and then implement a launchd recurring event (for the root account) to execute this script.

For information about how to set up a launchd recurring event, consult *Introduction to Command Line Administration*, available at www.apple.com/server/macosx/resources/.

A launchd recurring event should ensure that a specified time period (or less) should pass from the time a system update is applied and the ACL is reset. Because the ACL described above uses the `+a#` option to place rules in a noncanonical order, its reapplication results in additional rules. The following script can successfully apply – and reapply – the rules:

```
chmod -a "group:admin allow execute" <program name>
chmod +a "group:staff deny execute" <program name>
chmod +a# 0 "group:admin allow execute" <program name>
```

Securing User Home Folders

To secure user home folders, change the permissions of each user's home folder so the folder is not world-readable or world-searchable.

When FileVault is not enabled, permissions on the home folder of a user account allow other users to browse the folder's contents. However, users might inadvertently save sensitive files to their home folder, instead of into the more-protected `~/Documents`, `~/Library`, or `~/Desktop` folders.

The `~/Sites`, `~/Public`, and `~/Public/Drop Box` folders in each home folder may require world-readable or world-writeable permissions if File Sharing or Web Sharing is enabled. If these services are not in use, the permissions on these folders can be safely changed to prevent other users from browsing or writing to their contents.

As the owner of his or her home folder, the user can alter the folder's permission settings at any time, and can change these settings back.

In Snow Leopard Server all users are a member of the "staff" group, not of a group that has the same name as their user name.

Note: Changing permissions on a user's home directory from 750 to 700 will disable Apple file sharing (using the `~/Public` directory) and Apple web sharing (using the `~/Sites` directory).

To change home folder permissions:

- Enter the following command, replacing `username` with the name of the account:

```
sudo chmod 700 /Users/username
```

Run this command immediately after someone creates an account.

Encrypting Home Folders

Leopard includes FileVault, which can encrypt your home folder and its files. Use FileVault on portable computers and other computers whose physical security you can't guarantee. Enable FileVault encryption for your computer and its user accounts.

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

If you remove files from a FileVault-protected home folder it takes time to recover free space from the home folder. After the home folder is optimized, you can access files in FileVault-protected home folders without noticeable delays.

If you're working with confidential files that you plan to erase later, store those files in separate encrypted images that are not located in your home folder. You can then erase those images without needing to recover free space. For more information, see "Encrypting Portable Files" on page 155.

If you've insecurely deleted files before using FileVault, these files are recoverable after activating it. To prevent this, when you initially enable FileVault, securely erase free space. For information, see "Using Disk Utility to Securely Erase Free Space" on page 160.

Because FileVault is an encryption of a user's local home folder, FileVault does not encrypt or protect files transferred over the network or saved to removable media, so you'll need to encrypt specific files or folders. FileVault can only be enabled for local or mobile accounts and cannot be enabled for network home folders.

To protect files or folders on portable media or a network volume, create an encrypted disk image on the portable media or network volume. Then mount these encrypted disk images, which protect data transmitted over the network using AES-128 encryption. When using this method, mount the encrypted disk image from one computer at a time to prevent irreparable corruption to the image content.

For information about encrypting specific files or folders for transfer from your network home folder, see "Encrypting Portable Files" on page 155.

When you set up FileVault, you create a master password. If you forget your login password, you can use your master password to recover encrypted data. If you forget your login password and your master password, you cannot recover your data. Because of this, consider sealing your master password in an envelope and storing it in a secure location.

You can use Password Assistant to help create a complex master password that cannot be easily compromised. For information, see “Using Password Assistant to Generate or Analyze Passwords” on page 84.

Enabling FileVault copies data from your home folder into an encrypted home folder. After copying, FileVault erases the unencrypted data.

By default FileVault insecurely erases the unencrypted data, but if you enable secure erase, your unencrypted data is securely erased.

Overview of FileVault

Snow Leopard Server extends the unlocking of FileVault to Smart Cards, which provides the most secure practice for protecting FileVault accounts.

Accounts protected by FileVault support authentication using a passphrase or a Smart Card. With Smart Card authentication, the AES-256 symmetric Data Key (DK) used to encrypt the user’s data is unwrapped using a private (encryption) key on the Smart Card. The data written to or read from disk is encrypted and decrypted on the fly during access.

FileVault encrypts the Data Key (DK) using the User Key (UK1), which can be generated from your passphrase or from the public key on your Smart Card. FileVault separately encrypts the Data Key using the FileVault Master Key (MK).

The architectural design of FileVault makes it possible for the MK and UK1 to encrypt and decrypt files. Providing strong encryption protects user data at rest while ensuring access management by IT staff.

The easiest method for centralized management of FileVault on a client computer is to use Snow Leopard Server and WorkGroup Manager to enforce the use of FileVault and the proper identity.

Managing FileVault

You can set a FileVault master keychain to decrypt an account that uses FileVault to encrypt data. Then if users forget their FileVault account password (which they use to decrypt encrypted data) you can use the FileVault master keychain to decrypt the data.

To create the FileVault master keychain:

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

Select a strong password and consider splitting the password into at least two components (first half and second half). You can use Password Assistant to ensure that the quality of the password is strong.

To avoid having one person know the full password, have separate security administrators keep each password component. This prevents a single person from unlocking (decrypting) a FileVault account. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 84.

Setting a master password creates a keychain called FileVaultMaster.keychain in / Library/Keychains/. The FileVault master keychain contains a FileVault recovery key (self-signed root certificate) and a FileVault master password key (private key).

- 3 Delete the certificate named FileVaultMaster.cer in the same location as the FileVaultMaster.keychain.

FileVaultMaster.cer is only used for importing the certificate into the keychain. This is only a certificate and does not contain the private key, so there is no security concern about someone with gaining access to this certificate.

- 4 Make a copy of 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.

Deleting the key ensures that even if someone unlocks the FileVault master keychain they cannot decrypt the contents of a FileVault account because there is no FileVault master password private key available for the decryption.

Managing the FileVault Master Keychain

The modified FileVault master keychain can now be distributed to network computers. This can be done by transferring FileVaultMaster.keychain to the computers by using Apple Remote Desktop, by using a distributed installer executed on each computer, by using various scripting techniques, or by including it in the original disk image if your organization restores systems with a default image.

The master keychain provides network management of any FileVault account created on any computer with the modified FileVaultMaster.keychain located in the /Library/Keychains/ folder. These computers indicate that the master password is set in Security preferences.

When an account is created and the modified FileVault master keychain is present, the public key from the FileVault recovery key is used to encrypt the dynamically generated AES 128-bit (default) or AES 256-bit symmetric key that is used for the encryption and decryption of the encrypted disk image (FileVault container).

To decrypt access to the encrypted disk image, the FileVault master password private key is required to decrypt the original dynamically generated AES 128-bit or 256-bit symmetric key.

The user's original password continues to work as normal, but the assumption here is that the master password service is being used because the user has forgotten the password or the organization must perform data recovery from a user's computer.

To recover a network managed FileVault system account:

- 1 Retrieve the copy of FileVaultMaster.keychain that was stored before the private key was deleted during modification.
- 2 Bring together all security administrators involved in generating the master password.

More than one individual is needed if the master password was split into password components.

Note: The administrator must have root access to restore the FileVaultMaster.keychain file.

- 3 Restore the original keychain to the /Library/Keychains/ folder of the target computer, replacing the installed keychain.
- 4 Verify that the restored FileVaultMaster.keychain file has the correct ownership and permissions set, similar to the following example.

```
-rw-r--r-- 1 root admin 24880 Mar 2 18:18 FileVaultMaster.keychain
```

- 5 Verify that "Password Hints" is enabled by logging in to the FileVault account you are attempting to recover and incorrectly enter the account password three times.
If "Password Hints" is enabled, you are granted an additional try after the hint appeals.
- 6 When prompted for the master password, have the security administrators combine their password components to unlock access to the account.
- 7 When the account is unlocked, provide a new password for the account.
The password is used to encrypt the original symmetric key used to encrypt and decrypt the disk image.

Note: This process does not reencrypt the FileVault container. It reencrypts the original symmetric key with a key derived from the new user account password you entered.

You are now logged in to the account and given access to the user's home folder.

- 8 Delete the private key from FileVaultMaster.keychain again, or replace the keychain file with the original copy of FileVaultMaster.keychain that was stored before the private key was deleted.

This process does not change the password used to protect the user's original login keychain, because that password is not known or stored anywhere. Instead, this process creates a login keychain with the password entered as the user's new account password.

Encrypting Portable Files

To protect files you want to transfer over a network or save to removable media, encrypt a disk image or encrypt the files and folders. FileVault doesn't protect files transmitted over the network or saved to removable media.

Using a server-based encrypted disk image provides the added benefit of encrypting network traffic between the computer and the server hosting the mounted encrypted disk image.

Creating an Encrypted Disk Image

To encrypt and securely store data, you can create a read/write image or a sparse image:

- A read/write image consumes the space that was defined when the image was created. For example, if the maximum size of a read/write image is set to 10 GB, the image consumes 10 GB of space even if it contains only 2 GB of data.
- A sparse image consumes only the amount of space the data needs. For example, if the maximum size of a sparse image is 10 GB and the data is only 2 GB, the image consumes only 2 GB of space.

If an unauthorized administrator might access your computer, creating an encrypted blank disk image is preferred to creating an encrypted disk image from existing data.

Creating an encrypted image from existing data copies the data from an unprotected area to the encrypted image. If the data is sensitive, create the image before creating the documents. This creates the working copies, backups, or caches of files in encrypted storage from the start.

Note: To prevent errors when a file system inside a sparse image has more free space than the volume holding the sparse image, HFS volumes inside sparse images report an amount of free space slightly less than the amount of free space on the volume that the image resides on.

To create an encrypted disk image:

- 1 Open Disk Utility.
- 2 Choose File > New > Blank Disk Image.
- 3 Enter a name for the image, and choose where to store it.
- 4 Choose the size of the image by clicking the Size pop-up menu.
Make sure the size of the image is large enough for your needs. You cannot increase the size of an image after creating it.
- 5 Choose an encryption method by clicking the Encryption pop-up menu.
AES-128 or AES-256 is a strong encryption format.
- 6 Choose a format by clicking the Format pop-up menu.

Although there is some overhead, the sparse format allows the image to maintain a size proportional to its contents (up to its maximum size), which can save disk space.

- 7 Click Create.
- 8 Enter a password, and verify it.

You can access Password Assistant from this window. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 84.

- 9 Deselect “Remember password (add to Keychain),” and click OK.

Creating an Encrypted Disk Image from Existing Data

If you must maintain data confidentiality when transferring files from your computer but you don’t need to encrypt files on your computer, create a disk image from existing data.

Such situations include unavoidable plain-text file transfers across a network, such as mail attachments or FTP, or copying to removable media, such as a CD or floppy disk.

If you plan to add files to this image instead of creating an image from existing data, create an encrypted disk image and add your existing data to it. For information, see “Creating an Encrypted Disk Image” on page 155.

To create an encrypted disk image from existing data:

- 1 Open Disk Utility.
- 2 Choose File > New > Disk Image from Folder.
- 3 Select a folder and click Image.
- 4 Enter a name for the image and choose where to store it.
- 5 Choose a format 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.

- 6** Choose an encryption method by clicking the Encryption pop-up menu.
AES-128 or AES-256 provide strong encryption.
- 7** Click Save.
- 8** Enter a password and verify it.
You can easily access Password Assistant from this window. For more information, see “Using Password Assistant to Generate or Analyze Passwords” on page 84.
- 9** Deselect “Remember password (add to Keychain)” and click OK.
You can also use the `hdidutil` command to create and format encrypted disk images. For more information about this command, see its man page.

Creating Encrypted PDFs

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

Some applications do not support printing to PDF. In this case, create an encrypted disc image. For information, see “Creating an Encrypted Disk Image from Existing Data” on page 156.

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 Save as PDF.
- 4** Click Security Options and select one or more of the following options:
 - Require password to open document
 - Require password to copy text images and other content
 - Require password to print document

When you require a password for the PDF, it becomes encrypted.

- 5** Enter a password, verify it, and click OK.
- 6** Enter a name for the document, choose a location, and click Save.
- 7** Test your document by opening it.

You must enter the password before you can view the contents of your document.

Securely Erasing Data

When you erase a file, you're removing information that the file system uses to find the file. The file's location on the disk is marked as free space. If other files have not written over the free space, it is possible to retrieve the file and its contents.

Snow Leopard provides the following ways to securely erase files.

- Zero-out erase
- 7-pass erase
- 35-pass erase

A zero-out erase sets all data bits on the disk to 0, while a 7-pass erase and a 35-pass erase use algorithms to overwrite the disk. A 7-pass erase follows the Department of Defense standard for the sanitization of magnetic media. A 35-pass erase uses the extremely advanced Gutmann algorithm to help eliminate the possibility of data recovery.

The zero-out erase is the quickest. The 35-pass erase is the most secure, but it is also 35 times slower than the zero-out erase.

Each time you use a 7-pass or 35-pass secure erase, the following seven-step algorithm is used to prevent the data from being recovered:

- Overwrite file with a single character
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters

Configuring Finder to Always Securely Erase

In Snow Leopard Server you can configure Finder to always securely erase items placed in the Trash. This prevents data you place in the Trash from being restored. Using secure erase take longer than emptying the Trash.

To configure Finder to always perform a secure erase:

- 1 In Finder, choose Finder > Preferences.
- 2 Click Advanced.
- 3 Select the "Empty Trash securely" checkbox.

Using Disk Utility to Securely Erase a Disk or Partition

You can use Disk Utility to securely erase a partition, using a zero-out erase, a 7-pass erase, or a 35-pass erase.

Note: If you have a partition with Snow Leopard installed and you want to securely erase an unmounted partition, you don't need to use your installation discs. In the Finder, open Disk Utility (located in /Applications/Utilities/).

WARNING: Securely erasing a partition is irreversible. Before erasing the partition, back up critical files you want to keep.

To securely erase a partition using Disk Utility:

- 1 Insert the first of the Snow Leopard installation discs in the optical drive.
- 2 Restart the computer while holding down the C key.

The computer starts up from the disc in the optical drive.
- 3 Proceed past the language selection step.
- 4 Choose Utilities > Disk Utility.
- 5 Select the partition you want to securely erase.

Select a partition, not a drive. Partitions are contained in drives and are indented one level in the list on the left.
- 6 Click Erase, choose "Mac OS Extended Journaled," and then click Security Options.

Mac OS Extended disk formatting provides enhanced multiplatform interoperability.
- 7 Choose an erase option and click OK.
- 8 Click Erase.

Securely erasing a partition can take time, depending on the size of the partition and the method you choose.

Using Command-Line Tools to Securely Erase Files

You can use the `srm` command in Terminal to securely erase files or folders. By using `srm`, you can remove each file or folder by overwriting, renaming, and truncating the file or folder before erasing it. This prevents other people from undeleting or recovering information about the file or folder.

For example, `srm` supports simple methods, like overwriting data with a single pass of zeros, to more complex ones, like using a 7-pass or 35-pass erase.

The `srm` command cannot remove a write-protected file owned by another user, regardless of the permissions of the directory containing the file.

WARNING: Erasing files with `srm` is irreversible. Before securely erasing files, back up critical files you want to keep.

To securely erase a folder named secret:

```
sudo srm -r -s secret
```

The `-r` option removes the content of the directory, and the `-s` option (simple) overwrites with a single random pass.

For a more secure erase, use the `-m` (medium) option to perform a 7-pass erase of the file. The `-s` option overrides the `-m` option, if both are present. If neither is specified, the 35-pass is used.

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

Using Secure Empty Trash

Secure Empty Trash uses a 7-pass erase to securely erase files stored in the Trash. Depending on the size of the files being erased, securely emptying the Trash can take time to complete.

WARNING: Using Secure Empty Trash is irreversible. Before securely erasing files, back up critical files you want to keep.

To use Secure Empty Trash:

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

Using Disk Utility to Securely Erase Free Space

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

To securely erase free space using Disk Utility:

- 1 Open Disk Utility (located in /Applications/Utilities/).
- 2 Select the partition to securely erase free space from.

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

- 3 Click Erase, and then click Erase Free Space.

- 4 Choose an erase option and click Erase Free Space.

Securely erasing free space can take time, depending on the amount of free space being erased and the method you choose.

- 5 Choose Disk Utility > Quit Disk Utility.

Using Command-Line Tools to Securely Erase Free Space

You can securely erase free space from the command line by using the `diskutil` command. However, ownership of the affected disk is required. This tool allows you to securely erase using one of the three levels of secure erase:

- 1—Zero-out secure erase (also known as single-pass)
- 2—7-pass secure erase
- 3—35-pass secure erase

To erase free space using a 7-pass secure erase (indicated by the number 2):

```
sudo diskutil secureErase freespace 2 /dev/disk0s3
```

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

From the command line:

```
# -----
# Using Disk Utility to Securely Erase Free Space
# -----
# Overwrite a device with zeroes.
sudo diskutil zeroDisk /dev/device

# Secure erase (7-pass) free space on a volume.
sudo diskutil secureErase freespace 2 /dev/device

# Secure erase (7-pass) a volume.
sudo diskutil secureErase 2 /dev/device
```

Deleting Permanently from Time Machine Backups

Time Machine is based on the Mac OS X HFS+ file system. It tracks file changes and detects file system permissions and user access privileges.

When Time Machine performs the initial backup, it copies the contents of your computer to your backup drive. Every subsequent backup is an incremental backup, which copies only the files that have changed since the previous backup.

You can permanently delete files or folders from your computer and all Time Machine backups using Time Machine. This keeps sensitive data that you no longer need from being recovered.

To permanently delete files or folders from Time Machine backups:

- 1 Delete the file or folder from your computer.
 - 2 Open Time Machine.
 - 3 Select the file or folder you want to permanently delete from Time Machine.
 - 4 Click the Action pop-up menu and select "Delete All Backups of "*File or Folder name*."
 - 5 When the warning message appears, click OK to permanently delete the file or folder.
- All backup copies of your file or folder are permanently deleted from your computer.

Use this chapter to learn how Snow Leopard Server supports services that ensure encrypted data transfer through certificates.

Snow Leopard Server uses a Public Key Infrastructure (PKI) system to generate and maintain certificates of identities. Server Admin makes it easy to manage Secure Sockets Layer (SSL) certificates that can be used by web, mail, directory services, and other services that support them.

You can create a self-signed certificate and generate a Certificate Signing Request (CSR) to obtain an SSL certificate from an issuing authority and install the certificate.

For more information about how to use SSL certificates with individual services, see Chapter 10, “Setting General Protocols and Access to Services.” Also, for more information about certificates using the command line, see the man page of the `security` command-line tool.

Understanding Public Key Infrastructure

Snow Leopard Server supports services that use SSL to ensure encrypted data transfer. It uses a PKI system to generate and maintain certificates for use with SSL-enabled services.

PKI systems allow the two parties in a data transaction to be authenticated to each other, and to use encryption keys and other information in identity certificates to encrypt and decrypt messages traveling between them.

PKI enables multiple communicating parties to establish confidentiality, message integrity, and message source authentication without exchanging secret information in advance.

SSL technology relies on a PKI system for secure data transmission and user authentication. It creates an initial secure communication channel to negotiate a faster, secret key transmission. Snow Leopard Server uses SSL to provide encrypted data transmission for Mail, Web, and Directory services.

Public and Private Keys

Within a PKI, two digital keys are created: the public key and the private key. The private key isn't distributed to anyone and is often encrypted by a passphrase. The public key is distributed to other communicating parties.

Basic key capabilities can be summed up as:

Key type	Capabilities
Public	<ul style="list-style-type: none">• Can encrypt messages that can only be decrypted by the holder of the corresponding Private key.• Can verify the signature on a message to ensure that it is coming from a Private key.
Private	<ul style="list-style-type: none">• Can digitally sign a message or certificate, claiming authenticity.• Can decrypt messages that were encrypted with the Public key.• Can encrypt messages that can only be decrypted by the Private key itself.

Web, mail, and directory services use the public key with SSL to negotiate a shared key for the duration of the connection.

For example, suppose a mail server sends its public key to a connecting client and initiates negotiation for a secure connection. The connecting client uses the public key to encrypt a response to the negotiation. The mail server, because it has the private key, can decrypt the response. The negotiation continues until mail server and client have a shared secret to encrypt traffic between the two computers.

Certificates

A certificate is an electronic document that contains a public key with identification information (name, organization, email address, and so on). In a public key environment, a certificate is digitally signed by a Certificate Authority, or its own private key (the latter being a self-signed certificate).

A public key certificate is a file in a specified format (Mac OS X Server uses the x.509 format) that contains:

- The public key half of a public-private key pair
- The key user's identity information, such as a person's name and contact information
- A validity period (how long the certificate can be trusted to be accurate)
- The URL of someone with the power to revoke the certificate (its *revocation center*)
- The digital signature of a CA, or the key user

About Certificate Authorities (CAs)

A CA is an entity that signs and issues digital identity certificates claiming that a party is correctly identified. In this sense, a CA is a trusted third party used by other parties when performing transactions.

In x.509 systems such as Snow Leopard Server, CAs are hierarchical, with CAs being certified by higher CAs, until you reach a root authority. A root authority is a CA that's trusted by the parties, so it doesn't need to be authenticated by another CA. The hierarchy of certificates is top-down, with the root authority's certificate at the top.

A CA can be a company that signs and issues a public key certificate. The certificate attests that the public key belongs to the owner recorded in the certificate.

In a sense, a CA is a digital notary public. You request a certificate by providing the CA with your identity information, contact information, and the public key. The CA then verifies your information so users can trust certificates issued for you by the CA.

About Identities

Identities are a certificate and a private key, together. The certificate identifies the user, and the private key corresponds to the certificate. A single user can have several identities; for any given user each certificate can have a different name, email address, or issuer.

These identities are used for different security contexts. For example, one can be used to sign others' certificates, one can be used to identify the user by email, and these do not need to be the same identity.

In the context of the Mac OS X Server Certificate Manager, identities include a signed certificate and both keys of a PKI key pair. The identities are used by the system keychain and are available for use by services that support SSL.

Self-Signed Certificates

Self-signed certificates are certificates that are digitally signed by the private key corresponding to the public key included in the certificate. This is done in place of a CA signing the certificate. By self-signing a certificate, you're attesting that you are who you say you are. No trusted third party is involved.

About Intermediate Trust

If you are your own CA and your certificates are not trusted by the default shipping root certificates in Mac OS X, your clients can still be configured to trust your certificates through an intermediate trust.

Trust is the ability of a client to believe the identity of a server when it connects. A trusted server is a known server that the client can transact with securely, without interference from outside and unknown parties.

Mac OS X clients follow x.509 trust validation when accepting certificates, meaning they follow the chain of certificate signers back until they find a trusted root certificate.

Mac OS X lets you specify a trusted anchor (in other words, a certificate that is not a root CA certificate, but that you trust). A client can trust a certificate closer in the chain of trust, or even just the submitted certificate itself.

Trusting a certificate that isn't a shipping root anchor is intermediate trust. To accomplish this, trust needs to be bestowed on certificates instead of to keychains (as was done previously). In v10.4, trust was given to certificates in the keychain called "X509Anchors." The X509Anchors keychain was deprecated starting with Mac OS X v10.5.

In Snow Leopard Server, several keychains can hold certificates:

- **SystemRootCertificates:** This keychain holds root certificates that ship with Mac OS X. The certificates already have trust given to them.
- **System:** This keychain holds certificates that the computer administrator can add. All users on a given client can read from this keychain. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates.
- **Any other keychain:** This holds certificates for a given user and is only accessible to that user. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates or System.

Trusted certificates can be in any of these locations, but to trust a certificate, trust settings must be given explicitly to a certificate.

To configure clients to trust a certificate:

- 1 Copy the self-signed CA certificate (the file named ca.crt) onto each client computer. This is preferably distributed using nonrewritable media, such as a CD-R. Using nonrewritable media prevents the certificate from being corrupted.
- 2 Open the Keychain Access tool by double-clicking the ca.crt icon where the certificate was copied onto the client computer.
- 3 Drag the certificate to the System keychain using Keychain Access. Authenticate as an administrator, if requested.
- 4 Double-click the certificate to get the certificate details.
- 5 In the details window, click the Trust disclosure triangle.
- 6 From the pop-up menu next to "When using this certificate," select "Always Trust" You have now added trust to this certificate, regardless of who it is signed by.

From the command line

After copying the certificate to the target client computer, perform the following, replacing <certificate> with the file path to the certificate:

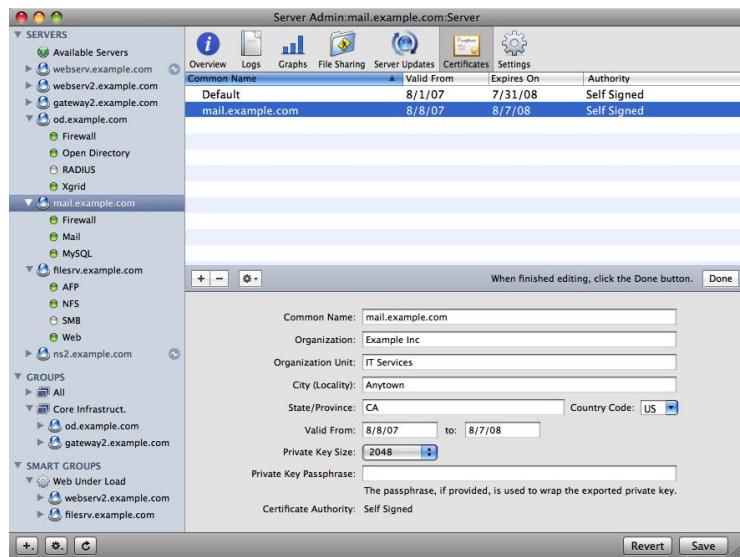
```
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/  
System.keychain <certificate>
```

You can use the security tool to save and restore trust settings as well. For more information on using the `security` command-line tool, see the `security` man page.

Certificate Manager in Server Admin

Snow Leopard Server's Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services.

The Server Admin interface is shown below, with the Certificate Manager selected.



Certificate Manager provides integrated management of SSL certificates in Snow Leopard Server for services that allow the use of SSL certificates. On installation, the server creates a self-signed certificate for immediate use from information you put in during server setup.

Certificate Manager uses Mac OS X's Certificate Assistant to create self-signed certificates and certificate-signing requests (CSRs) to obtain certificates signed by a CA. The certificates, self-signed or signed by a CA, are then accessible by services that support SSL.

Certificate Manager in Server Admin doesn't allow you to sign and issue certificates as a CA, nor does it allow you to sign and issue certificates as a root authority. If you need these functions, you can use Certificate Assistant in Keychain Access (located in /Applications/Utilities/). It provides these capabilities and others for working with x.509 certificates.

Identities that were created and stored in OpenSSL files can also be imported into Certificate Manager. They are accessible to services that support SSL. Self-signed and CA-issued certificates you created in CA Assistant can be used in Certificate Manager by importing the certificate.

Certificate Manager displays the following for each certificate:

- The domain name the certificate was issued for
- The expiration date of the certificate
- When selected, the detailed contents of the certificate

When certificates and keys are imported via Certificate Manager, they are put in the /etc/certificates/ directory. The directory contains four PEM formatted files for every identity:

- The certificate
- The public key
- The trust chain
- The concatenated version of the certificate plus the trust chain (for use with some services)

The certificate and trust chain are owned by the root user and the wheel group, with permissions set to 644. The public key and concatenation file are owned by the root user and the certusers group, with permissions set to 640.

Each file has the following naming convention:

<common name>.<SHA1 hash of the certificate>.<cert | chain | concat | key>.pem

For example, the certificate for a web server at example.com might look like this:

www.example.com.C42504D03B3D70F551A3C982CFA315595831A2E3.cert.pem

Readyng Certificates

Before you can use SSL in Mac OS X Server's services, you must create or import certificates. You can create self-signed certificates, create certificates and then generate a Certificate Signing Request (CSR) to send to a CA, or import certificates previously created with OpenSSL.

If you have previously generated certificates for SSL, you can import them for use by Mac OS X Server services. The OpenSSL keys and certificates must be in PEM format.

Select a CA to sign your certificate request. If you don't have a CA to sign your request, consider becoming your own CA and then import your CA certificates into the root trust database of your managed machines.

When you set up Mac OS X Server, the Server Assistant creates a self-signed certificate based on information you provided when it's first installed. It can be used for any service that supports SSL. When your clients choose to trust the certificate, SSL connections can be used without user interaction from that point on.

This initial self-signed certificate is used by Server Admin and Server Preferences to encrypt administrative functions.

Creating a Self-Signed Certificate

A self-signed certificate is generated at server setup. Although it is available for use, you may want to customize the information in the certificate, so you would create a new self-signed certificate. This is especially important if you plan on having a CA sign your certificate.

When you create a self-signed certificate, Certificate Manager creates a private-public key pair in the System keychain with the key size specified (512 - 2048 bits). It then creates the corresponding self-signed certificate.

If you're using a self-signed certificate, consider using an intermediate trust for it and import the certificate into the System keychain on all client computers (if you have control of the computers). For more information about using intermediate trust, see "About Intermediate Trust" on page 165.

To create a self-signed certificate:

- 1 In Server Admin, select the server that has services that support SSL.
 - 2 Click Certificates.
 - 3 Click the Add (+) button and choose Create a Certificate Identity.
- Certificate Assistant launches, populated with information needed to generate the certificate.
- 4 If you override the defaults, choose "Let me override defaults" and follow the onscreen instructions.
 - 5 When finished, click Continue.
 - 6 Confirm the certificate creation by clicking Continue.

The Certificate Assistant generates a key pair and certificate. Certificate Manager encrypts the files with a random passphrase, puts the passphrase in the System keychain, and puts the resulting PEM files in /etc/certificates/.

Storing the Private Key

The private key should be generated on a computer that is not connected to your internal network. For added security, you can store the keychain containing the private key on USB storage so you can keep the CA private key unavailable when connected to the network.

Requesting a Certificate from a CA

Certificate Manager helps you create a CSR to send to your designated CA.

You need a certificate for the CA to sign. You can use the one that was generated at server setup, but more likely you will want to generate one that has all the details the CA requires before signing. If you need to generate a certificate before getting it signed, see “Creating a Self-Signed Certificate” on page 169.

To request a signed certificate:

- 1 In Server Admin, select the server that has services that support SSL.
- 2 Click Certificates.
- 3 Select the certificate you want signed.
- 4 Click the Action button below the certificates list and choose “Generate Certificate Signing Request (CSR).”
- 5 Certificate manager creates the signing request and shows the ASCII text version in the sheet.
- 6 Click Save to save the CSR to the disk.

Your CA will have instructions on how to transfer the CSR to the signer. Some CAs require you to use a web interface; others require sending the CSR in the body of a mail message. Follow the instructions given by the CA.

The CA will return a newly signed certificate, which replaces the one you generated. For instructions on what to do now with your newly signed certificate, see “Replacing an Existing Certificate” on page 175.

Creating a CA

To sign another user’s certificate, you must create a CA. Sometimes a CA certificate is referred to as a root or anchor certificate. By signing a certificate with the root certificate, you become the trusted third party in that certificate’s transactions, vouching for the identity of the certificate holder.

If you are a large organization, you might decide to issue or sign certificates for people in your organization to use the security benefits of certificates. However, external organizations might not trust or recognize your signing authority.

To create a CA:

- 1 Start Keychain Access.

Keychain Access is found in the /Applications/Utilities/ directory.

- 2 In the Keychain Access menu, select Certificate Assistant > Create a Certificate Authority.

The Certificate Assistant starts. It will guide you through the process of making the CA.

- 3 Choose to create a Self Signed Root CA.

- 4 Provide the Certificate Assistant with the requested information and click Continue.

You need the following information to create a CA:

- An email address
- The name of the issuing authority (you or your organization)

You also decide if you want to override the defaults and whether to make this CA the organization's default CA. If you do not have a default CA for the organization, allow the Certificate Assistant to make this CA the default.

In most circumstances, do not override the defaults. If you do not override the defaults, skip to step 16.

- 5 If you override the defaults, provide the following information in the next few screens:

- A unique serial number for the root certificate
- The number of days the CA functions before expiring
- The type of user certificate this CA is signing
- Whether to create a CA website for users to access for CA certificate distribution

- 6 Click Continue.

- 7 Provide the Certificate Assistant with the requested information and click Continue.

You need the following information to create a CA:

- An email address of the responsible party for certificates
- The name of the issuing authority (you or your organization)
- The organization name
- The organization unit name
- The location of the issuing authority

- 8 Select a key size and an encryption algorithm for the CA certificate, and then click Continue.

A larger key size is more computationally intensive to use, but much more secure. The algorithm you choose depends more on your organizational needs than a technical consideration.

DSA and RSA are strong encryption algorithms. DSA is a United States Federal Government standard for digital signatures.

- 9 Select a key size and an encryption algorithm for the certificates to be signed, and then click Continue.
- 10 Select the Key Usage Extensions you need for the CA certificate, and then click Continue.

At a minimum, you must select Signature and Certificate Signing.
- 11 Select the Key Usage Extensions you need for the certificates to be signed, and then click Continue.

Default key use selections are based on the type of key selected earlier in the Assistant.
- 12 Specify other extensions to add the CA certificate and click Continue.
- 13 Select the keychain “System” to store the CA certificate.
- 14 Choose to trust certificates on this computer signed by the created CA.
- 15 Click Continue and authenticate as an administrator to create the certificate and key pair.
- 16 Read and follow the instructions on the last page of the Certificate Assistant.

You can now issue certificates to trusted parties.

Importing a Certificate Identity

You can import a previously generated OpenSSL certificate and private key into Certificate Manager. The items are listed as available in the list of identities and are available to SSL-enabled services.

The OpenSSL keys and certificates must be in PEM format.

To import an existing OpenSSL style certificate:

- 1 In Server Admin, select the server that has services that support SSL.
- 2 Click Certificates.
- 3 Click the Add (+) button and choose Import a Certificate Identity.
- 4 Drag the PEM file containing the private key to the sheet.
- 5 Drag the PEM file containing the public certificate to the sheet.
- 6 If needed, drag associated nonidentity certificates to the sheet as well.
- 7 Click the Import button.

If prompted, enter the private key passphrase.

Managing Certificates

After you create and sign a certificate, you won't do much more with it. Because certificates cannot be edited, you can delete, replace, or revoke certificates after they are created. You cannot change certificates after a CA signs them.

If the information a certificate possesses (such as contact information) is no longer accurate, or if you believe the private key is compromised, delete the certificate.

If you have previously generated certificates for SSL, you can import them for use by services. The OpenSSL keys and certificates must be in PEM format.

If you chose custom locations for your SSL certificates with Snow Leopard Server, you must import them into Certificate Manager if you want them to be available for services.

Custom filesystem locations for certificates cannot be managed for services using Server Admin for Snow Leopard Server. To use custom file locations, edit the configuration files directly.

When certificates and keys are imported via Certificate Manager, they are put in the /etc/certificates/ directory. The directory contains four PEM formatted files for every identity:

- The certificate
- The public key
- The trust chain
- The concatenated version of the certificate plus the trust chain (for use with some services)

Each file has the following naming convention:

<common name>.<SHA1 hash of the certificate>.<cert | chain | concat | key>.pem

For example, the certificate for a web server at example.com might look like this:

www.example.com.C42504D03B3D70F551A3C982CFA315595831A2E3.cert.pem

After the certificates are imported, Certificate Manager encrypts the files with a random passphrase. It puts the passphrase in the System keychain, and puts the resulting PEM files in /etc/certificates/.

Editing a Certificate

After you add a certificate signature, you can't edit the certificate. You must replace it with one generated from the same private key.

For instructions on how to do this, see "Replacing an Existing Certificate" on page 175.

Distributing a CA Public Certificate to Clients

If you're using self-signed certificates, a warning appears in most user applications saying that the CA is not recognized. Other software, such as the LDAP client, refuses to use SSL if the server's CA is unknown.

Mac OS X Server ships only with certificates from well-known commercial CAs. To prevent this warning, your CA certificate must be distributed to every client computer that connects to the secure server.

To distribute your certificate to your clients:

- 1 Copy the self-signed CA certificate (the file named ca.crt) onto each client computer. Consider using nonrewritable media, such as a CD-R. Using nonrewritable media prevents the certificate from being corrupted.
- 2 Open the Keychain Access tool by double-clicking the ca.crt icon where the certificate was copied onto the client computer.
- 3 Drag the certificate to the System keychain using Keychain Access.
- 4 Authenticate as an administrator, if requested.
- 5 Double-click the certificate to get the certificate details.
- 6 In the details window, click the Trust disclosure triangle.
- 7 From the pop-up menu next to "When using this certificate," select "Always Trust."

You have now added trust to this certificate, regardless of who it is signed by.

From the command line:

```
# -----
# Adding the security tool edit trust settings
# -----
# Where <certificate> is the local file path to the certificate.
#
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/
System.keychain <certificate>
```

Deleting a Certificate

When a certificate has expired or been compromised, you must delete it.

To delete a certificate:

- 1 In Server Admin, select the server that has services that support SSL.
- 2 Click Certificates.
- 3 Select the Certificate Identity to delete.
- 4 Click the Remove (-) button and select Delete.

- 5 Click Save.

Renewing an Expiring Certificate

Certificates have an expiration date and must be renewed periodically. Renewing a certificate is the same as replacing a certificate with a newly generated one with an updated expiration date.

To renew an expiring certificate:

- 1 Request a certificate from the CA.
If you are your own CA, create one using your own root certificate.
- 2 In Server Admin in the Server list, select the server that has the expiring certificate.
- 3 Click Certificates.
- 4 Select the Certificate Identity to renew.
- 5 Click the Action button and select “Replace Certificate with Signed or Renewed Certificate.”
- 6 Drag the renewed certificate to the sheet.
- 7 Click Replace Certificate.

Replacing an Existing Certificate

If you change the DNS name of the server or any virtual hosts on the server, you must replace an existing certificate with an updated one.

To replace an expiring certificate:

- 1 Request a certificate from the CA.
If you are your own CA, create one using your own root certificate.
- 2 In Server Admin in the Server list, select the server that has the expiring certificate.
- 3 Click Certificates.
- 4 Select the Certificate Identity to replace.
- 5 Click the Action button and select “Replace Certificate with Signed or Renewed Certificate.”
- 6 Drag the replacement certificate to the sheet.
- 7 Click Replace Certificate.

Setting General Protocols and Access to Services

Use this chapter to learn how to use Server Admin to configure access to services and to set general protocols.

Server Admin helps you configure and manage servers. You can set general protocols, name or rename computers, set the date and time, manage certificates, and set user access to specific services.

Setting General Protocols

Snow Leopard Server includes basic network management protocols, including network time protocol (NTP) and simple network management protocol (SNMP). Unless these are required, they should be disabled.

Disabling NTP Service

NTP allows computers on a network to synchronize Date & Time settings. Client computers specify their NTP server in the Date & Time panel of System Preferences.

NTP client access is typically required. If so, enable it on a single, trusted server on the local network. This service should be disabled on all other servers.

For more information about the open source implementation, see www.ntp.org.

To disable NTP service:

- 1 Open Server Admin and connect to the server.
- 2 Click Settings, then click Date & Time.
- 3 Unless NTP is not required, make sure your server is configured to “Set date & time automatically.”
- 4 From the pop-up menu, choose the server you want to act as a time server.
- 5 Click General.
- 6 Deselect the “Network Time Server (NTP)” checkbox.
- 7 Click Save.

From the command line:

```
# -----
# Setting General Protocols
# -----



#
# Disable NTP Client access.
# -----
sudo systemsetup -setusingnetworktime off

#
# Disable NTP service.
#-----
sudo serveradmin settings info:ntpTimeServe = no
```

Disabling SNMP

SNMP software allows other computers to monitor and collect data on the state of a computer running Snow Leopard Server. This helps administrators identify computers that warrant attention, but use of this service is not recommended.

To disable SNMP:

- 1 Open Server Admin and connect to the server.
- 2 Click Settings.
- 3 Click General.
- 4 Deselect “Network Management Server (SNMP).”
- 5 Click Save.

From the command line:

```
# 
# Disable SNMP.
# -----


sudo serveradmin settings info:enableSNMP = no

# or alternatively.
#sudo service org.net-snmp.snmpd stop
```

Enabling SSH

Snow Leopard Server also includes secure shell (SSH). SSH allows you to log in to other computers on a network, execute commands remotely, and move files from one computer to another. It provides strong authentication and secure communication, and is therefore recommended if remote login is required. For more information, see www.openssh.org.

To enable SSH:

- 1 Open Server Admin and connect to the server.
- 2 Click Settings.
- 3 Click General.
- 4 Select “Remote Login (SSH).”
- 5 Click Save.

From the command line:

```
#  
# Enable SSH.  
# -----  
sudo service ssh start  
  
# or alternatively.  
# sudo serveradmin settings info:enableSSH = yes
```

About Remote Management (ARD)

You can use ARD to perform remote management tasks such as screen sharing. When sharing your screen provide access only to specific users to prevent unauthorized access to your computer screen. You must also determine the privileges users will have when viewing your screen.

ARD is turned off by default and should remain off when it is not being used. This prevents unauthorized users from attempting to access your computer.

You can administer ARD using a built-in command-line tool called kickstart. You can find more information about the tool and its capabilities by using its built-in help. Access the help by entering the following command:

```
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/  
Resources/kickstart -help
```

For more information about ARD and its uses and capabilities, see *Apple Remote Desktop Administrator Guide*.

Remote Management Best Practices

An ARD manager with full privileges can run these tasks as the root user. By limiting the privileges that an ARD manager has, you increase security. When setting privileges, disable or limit an administrator's access to an ARD client.

You can set a VNC password that requires authorized users to use a password to access your computer. The most secure way is to require authorized users to request permission to access your computer screen.

Remote Management can act as a standard VNC server, accepting connections from VNC clients. Enabling VNC access is not recommended.

If users connect to your computer using VNC, require that they use a password by enabling "VNC viewer may control screen with password." Use Password Assistant to create a strong password for VNC users.

Limiting Remote Management Access

Users that have access to screen control and command-line code execution using Apple Remote Desktop effectively have root user access on the computer, even if their user account is a standard account. You should limit what users are allowed to do with Remote Management.

Change the default setting for remote management from "All users" to "Only these users." The default setting "All users" includes all users on your local computer and all users in the directory server you are connected to.

Any account using ARD should have limited privileges to prevent remote users from having full control of your computer.

You can securely configure ARD by restricting access to specific users. You can also restrict each user's privileges by setting ARD options. Limit the user's privileges to the user's permission on the computer. For example, you might not want to give a standard user the ability to change your settings or delete items.

To Limit Remote Management Access:

- 1 On the server, open System Preferences and click Sharing.

If the preference pane is locked, click the lock and enter the user name and password of a user with administrator privileges on the computer.

- 2 Select Remote Management in the Sharing pane.
- 3 Select "Only these users," click Add (+), select users, and click Select.
- 4 Select a user in the list to change that user's administrator privileges.
- 5 Click Options.
- 6 Make the changes to the access privileges and then click OK.

Your changes take effect immediately.

You can hold down the Option key while clicking an access privilege checkbox to automatically select all access checkboxes.

For more information about the privileges list, see “Apple Remote Desktop Administrator Access” in the see *Apple Remote Desktop Administrator Guide*.

- 7 If you’re changing access for several users, repeat this for each user.

From the command line:

```
#  
# Remote Management (ARD)  
# -----  
# Limiting Remote Management Access  
# Repeat for each specified user.  
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/  
    Resources/kickstart -activate -configure -access -on -users  
    $ARD_USERNAME -privs -  
    <none|all|ControlObserve|DeleteFiles|ControlObserve|TextMessages>ShowO  
    bserve|OpenQuitApps|GenerateReports|RestartShutdown|SendFiles|ChangeSe  
    ttings|ObserveOnly> -restart  
# Specify the user  
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/  
    Resources/kickstart -allowAccessFor -specifiedUsers $ARD_USERNAME
```

Disabling Remote Management Access

You can disable Remote Management in several different ways. You can:

- Disable access for all users.
- Stop the ARD Agent process temporarily.
- Disable the service entirely.

You might want to keep the computer running as an ARD Task Server but not let users control it remotely. In such a case, you would disable access for the users, but leave the agent running and the service intact.

If you stop the agent, it relaunches at system restart, so it doesn’t remain permanently disabled.

To disable access for all users:

- 1 On the server, open System Preferences and click Sharing.

If the preference pane is locked, click the lock and enter the user name and password of a user with administrator privileges on the computer.

- 2 Select Remote Management in the Sharing pane.
- 3 Select a user from the “Only these users” list.

- 4 Click Remove (-).
- 5 Repeat for each user.

To stop the Agent process:

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

```
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
      Resources/kickstart -agent -stop
```

To disable the service:

- 1 Open Server Admin and connect to the server.
- 2 Click Settings.
- 3 Click General.
- 4 Deselect "Remote Management."
- 5 Click Save.

From the command line:

```
#  
## Disable Remote Management  
# -----  
# To remove user access:  
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
      Resources/kickstart -activate -configure -access -off  
  
# To stop the ARD agent:  
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
      Resources/kickstart -agent -stop  
  
# To disable the service:  
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
      Resources/kickstart -deactivate -stop  
  
#or alternatively.  
# sudo serveradmin settings info:enableARD = no
```

Remote Apple Events (RAE)

If you enable Remote Apple Events (RAE), you allow your computer to respond to events sent by other computers on your network. These events include AppleScript programs. A malicious AppleScript program can do things like delete your ~/Documents/ folder.

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

From the command line:

```
#  
# Remote Apple Events (RAE)  
# -----  
# Disable Remote Apple Events.  
sudo launchctl unload -w /System/Library/LaunchDaemons/eppc.plist
```

Restricting Access to Specific Users

Avoid enabling RAE. If you enable RAE, do so on a trusted private network and disable it immediately after disconnecting from the network. Change the default setting for RAE from “All users” to “Only these users.” The default setting “All users” includes all users on your local computer and all users in the directory server you are connected to.

When securely configuring RAE, restrict remote events to only be accepted from specific users. This prevents unauthorized users from sending malicious events to your computer. If you create a sharing user account, create a strong password using Password Assistant. Avoid accepting events from Mac OS 9 computers. If you need to accept Mac OS 9 events, use Password Assistant to create a strong password.

Setting the Server’s Host Name

You can change your computer name and local host name in Server Admin. When other users use Bonjour to discover your available services, the server is displayed as *hostname.local*.

To increase your privacy, change the host name of your computer so your computer cannot be easily identified. The name should not indicate the purpose of the computer, and the word “server” should not be used as the name or part of the name.

Setting the Date and Time

Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues. You can use Server Admin to configure your computer to set the date and time based on an NTP server. If you require automatic date and time, use a trusted, internal NTP server.

Setting Up Certificates

Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services. Certificate Manager provides integrated management of SSL certificates in Snow Leopard Server for services that allow the use of SSL certificates.

For more information about setting up certificates, see “Certificate Manager in Server Admin” on page 167.

Setting Service Access Control Lists (SACLs)

You use a Service Access Control List (SACL) to enforce who can use a specific service. It is not a means of authentication. It is a list of those who have access rights to use the service.

SACLs allow you to add a layer of access control on top of standard and ACL permissions.

A user or group not in a service’s SACL cannot access the service. For example, to prevent users from accessing AFP share points on a server, including home folders, remove the users from the AFP service’s SACL.

Server Admin in Snow Leopard Server allows you to configure SACLs. Open Directory authenticates user accounts, and SACLs authorize use of services. If Open Directory authenticates you, the SACL for the login window determines whether you can log in, the SACL for AFP service determines whether you can connect for Apple file service, and so on.

Some services also determine whether a user is authorized to access specific resources. This authorization can require retrieving additional user account information from the directory domain. For example, AFP service needs the user ID and group membership information to determine which folders and files the user is authorized to read and write to.

To set SACL permissions for a service:

- 1 Open Server Admin and connect to the server.
- 2 Click Access.
- 3 Click Services
- 4 To restrict access to all services or to deselect this option to set access permissions per service, select “For all services.”
- 5 If you deselect “For all services,” select a service from the Service list.
- 6 To provide unrestricted access to services, click “Allow all users and groups.”
To provide access to specific users and groups:

- a** Select “Allow only users and groups below.”
 - b** Click the Add (+) button to open the Users & Groups drawer.
 - c** Drag users and groups from the Users & Groups drawer to the list.
- 7** Click Save.

You can limit access to command-line tools that might run services by limiting the use of the `sudo` command. For more information, see “Managing the sudoers File” on page 361.

From the command line:

```
# Set SACL permissions for a service.  
# -----  
sudo dseditgroup -o edit -a $USER -t user $SACL_GROUP
```

Use this chapter to learn how to secure Remote Access services.

Many organizations have individuals who need to connect to network resources remotely. This can create additional vulnerabilities unless your remote access services are securely configured.

Snow Leopard Server allows remote access using remote login and VPN services. These services should be disabled unless they are required.

Remote Access services via remote login consists of two components each using the Secure Shell (SSH) service to establish an encrypted tunnel between client and server. “Securing Remote SSH Login” on page 185 discusses securing the server component, while “Configuring SSH” on page 186 discusses securing the client component.

For additional information about configuring remote access services, see the *Network Services Administration* guide.

Securing Remote SSH Login

Remote Login allows users to connect to your computer through SSH. By enabling Remote Login, you activate more secure versions of commonly used insecure tools.

Be aware of the following SSH tools:

- **sshd:** Daemon that acts as a server to all other commands
- **ssh:** Primary user tool for remote shell and port-forwarding sessions
- **scp:** Secure copy, a tool for automated file transfers
- **sftp:** Secure FTP, a replacement for FTP

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

SSH creates a secure encrypted channel that protects communication with your computers. Do not use older services that do not encrypt their communications, such as Telnet or RSH—they allow network eavesdroppers to intercept passwords or other data.

Unless you must remotely log in to the computer or use another program that depends on SSH, disable the remote login service. However, Server Admin requires SSH. If you disable remote login, you cannot use Server Admin to remotely administer the server.

To disable remote login:

- 1 Open System Preferences.
- 2 Click Sharing.
- 3 In the Service list, deselect Remote Login.

Configuring SSH

SSH lets you send secure, encrypted commands to a remote computer, as if you were sitting at the computer. Use the `ssh` tool in Terminal to open a command-line connection to a remote computer. While the connection is open, commands you enter are performed on the remote computer.

Note: You can use any application that supports SSH to connect to a computer running Snow Leopard or Snow Leopard Server.

SSH works by setting up encrypted tunnels using public and private keys. Here is a description of an SSH session:

- 1 The local and remote computers exchange their public keys.
If the local computer has never encountered a given public key before, SSH prompts you whether to accept the unknown key.
- 2 The two computers use the public keys to negotiate a session key that is used to encrypt subsequent session data.

- 3 The remote computer attempts to authenticate the local computer using RSA or DSA certificates. If this is not possible, the local computer is prompted for a standard user-name/password combination.

For information about setting up certificate authentication, see “Generating Key Pairs for Key-Based SSH Connections” on page 187.

- 4 After successful authentication, the session begins. Either a remote shell, a secure file transfer, a remote command, or so on, begins through the encrypted tunnel.

Modifying the SSH Configuration File

Making changes to the SSH configuration file enables you to set options for each ssh connection. You can make these changes systemwide or for specific users. To make the change systemwide, change the options in the /etc/ssh_config file, which affects ssh users on the computer. To make the change for a single user, change the options in the *username/.ssh/config* file.

The ssh configuration file has connection options and other specifications for an ssh host. A host is specified by the Host declaration. By default, the Host declaration is an asterisk (*), indicating that any host you are connecting to will use the options listed below the Host declaration.

You can add a specific host and options for that host by adding a new Host declaration. The new Host declaration will specify a name or address in place of the asterisk. You can then set the connection option for the host below the Host declaration. This helps secure your ssh sessions in environments with varying security levels.

For example, if you are connecting to a server using ssh through the Internet, the server might require a more secure or stricter connection. However, if you are in a more secure environment, such as your own personal network, you cannot require the same strict connection options.

For more information about ssh configuration file options, see the ssh man pages.

To enable SSH, see “Enabling SSH” on page 178.

Generating Key Pairs for Key-Based SSH Connections

By default, SSH supports the use of password, key, and Kerberos authentication. The standard method of SSH authentication is to supply login credentials in the form of a user name and password. Identity key pair authentication enables you to log in to the server without supplying a password.

This process works as follows:

- 1 A private and a public key are generated, each associated with a user name to establish that user’s authenticity.
- 2 When you attempt to log in as that user, the user name is sent to the remote computer.

- 3** The remote computer looks in the user's .ssh/ folder for the user's public key.
This folder is created after using SSH the first time.
- 4** A challenge is then sent to the user based on his or her public key.
- 5** The user verifies his or her identity by using the private portion of the key pair to decode the challenge.
- 6** After the challenge is decoded, the user is logged in without the need for a password.
This is especially useful when automating remote scripts.

Key-based authentication requires possession of the private key instead of a password to log in. A private key is much harder to guess than a password. However, if the home folder where the private key is stored is compromised—assuming the private key is not protected by a password—then this private key can be used to log in to other systems. Password authentication can be compromised without needing a private key file.

If the server uses FileVault to encrypt the home folder of the user you want to use SSH to connect as, you must be logged in on the server to use SSH. Alternatively, you can store the keys for the user in a location that is not protected by FileVault. However, this is not secure.

To generate the identity key pair:

- 1** Enter the following command on the local computer.
`ssh-keygen -t dsa`
- 2** When prompted, enter a filename to save the keys in the user's folder.
- 3** Enter a password followed by password verification (empty for no password).

For example:

```
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/anne/.ssh/id_dsa): frog
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in frog.
Your public key has been saved in frog.pub.
The key fingerprint is:
4a:5c:6e:9f:3e:35:8b:e5:c9:5a:ac:00:e6:b8:d7:96 annejohnson1@mac.com
```

This creates two files. Your identification or private key is saved in one file (frog in our example) and your public key is saved in the other (frog.pub in our example). The key fingerprint, derived cryptographically from the public key value, is also displayed. This secures the public key, making it computationally infeasible for duplication.

Note: The location of the server SSH key is /etc/ssh_host_key.pub. Back up your key in case you need to reinstall your server software. If your server software is reinstalled, you can retain the server identity by putting the key back in its folder.

- 4 Copy the resultant public file, which contains the local computer's public key, to the .ssh/ folder in the user's home folder on the remote computer.

The next time you log in to the remote computer from the local computer, you won't need to enter a password (unless you entered one in Step 3 above).

Note: If you are using an Open Directory user account and have logged in using the account, you do not need to supply a password for SSH login. On Snow Leopard Server computers, SSH uses Kerberos for single sign-on authentication with any user account that has an Open Directory password (but Kerberos must be running on the Open Directory server). For more information see the *Open Directory Administration*.

Updating SSH Key Fingerprints

The first time you connect to a remote computer using SSH, the local computer prompts for permission to add the remote computer's fingerprint (or encrypted public key) to a list of known remote computers. You might see a message like this:

```
The authenticity of host "server1.example.com" can't be established.  
RSA key fingerprint is a8:0d:27:63:74:f1:ad:bd:6a:e4:0d:a3:47:a8:f7.  
Are you sure you want to continue connecting (yes/no)?
```

The first time you connect, you have no way of knowing whether this is the correct host key. When you respond "yes," the host key is then inserted into the ~/.ssh/known_hosts file so it can be compared in later sessions. Be sure this is the correct key before accepting it. If at all possible, provide users with the encryption key through FTP, mail, or a download from the web, so they can verify the identity of the server.

If you later see a warning message about a man-in-the-middle attack when you try to connect, the key on the remote computer might no longer match the key stored on the local computer. This can happen if you:

- Change your SSH configuration on the local or remote computer.
- Perform a clean installation of the server software on the computer you are attempting to log in to using SSH.
- Start up from a Snow Leopard Server CD on the computer you are attempting to log in to using SSH.
- Attempt to use SSH to log in to a computer that has the same IP address as a computer that you previously used SSH with on another network.

To connect again, delete the entries corresponding to the remote computer you are accessing (which can be stored by both name and IP address) in ~/.ssh/known_hosts.

Important: Removing an entry from the known_hosts file bypasses a security mechanism that helps you avoid imposters and man-in-the-middle attacks. Be sure you understand why the key on the remote computer has changed before you delete its entry from the known_hosts file.

Controlling Access to SSH

You can use Server Admin to control which users can open a command-line connection using the `ssh` tool in Terminal. Users with administrator privileges are always allowed to open a connection using SSH. The `ssh` tool uses the SSH service.

For information about restricting user access to services, see “Setting Service Access Control Lists (SACLs)” on page 183.

SSH Man-in-the-Middle Attacks

An attacker might be able to access your network and compromise routing information, so that packets intended for a remote computer are routed to the attacker who impersonates the remote computer to the local computer and the local computer to the remote computer.

Here's a typical scenario: A user connects to the remote computer using SSH. By means of spoofing techniques, the attacker poses as the remote computer and receives the information from the local computer. The attacker then relays the information to the intended remote computer, receives a response, and then relays the remote computer's response to the local computer. Throughout the process, the attacker is aware of information that goes back and forth, and can modify it.

The following message can indicate a man-in-the-middle attack when connecting to the remote computer using SSH.

oo
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
oo

Protect against this type of attack by verifying that the host key sent back is the correct host key for the computer you are trying to reach. Be watchful for the warning message, and alert your users to its meaning.

Transferring Files Using SFTP

SFTP is a secure FTP protocol that uses SSH to transfer files. SFTP encrypts commands and data, preventing passwords and sensitive information from being transmitted over the network. Always use SFTP instead of FTP.

To transfer a file using SFTP:

- 1 Open Terminal.

- 2 Start the SFTP session.

```
sftp username@hostname
```

Replace *username* with your user name and *hostname* with the IP address or host name of the server you are connecting to.

- 3 Enter your password when prompted.

You are now connected securely to the server.

- 4 Use the SFTP commands to transfer files from the prompt.

```
sftp>
```

Use the `put` command to transfer a file from the local computer to the remote computer. Use the `get` command to transfer a file from the remote computer to the local computer.

- 5 Enter the following to transfer a picture file from the remote computer to the local computer.

```
sftp> get picture.png /users/annejohnson picture.png
```

- 6 To disconnect and end the SFTP session, enter `exit` at the prompt.

Securing VPN Service

By configuring a Virtual Private Network (VPN) on your server, you can give users a more secure way of remotely communicating with computers on your network.

A VPN consists of computers or networks (nodes) connected by a private link of encrypted data. This link simulates a local connection, as if the remote computer were attached to the LAN.

VPNs securely connect users working away from the office (for example, at home) to the LAN through a connection such as the Internet. From the user's perspective, the VPN connection appears as a dedicated private link.

VPN technology can also connect an organization to branch offices over the Internet while maintaining secure communications. The VPN connection across the Internet acts as a WAN link between the sites.

VPNs have several advantages for organizations whose computer resources are physically separated. For example, each remote user or node uses the network resources of its Internet Service Provider (ISP) rather than having a direct, wired link to the main location.

VPN and Security

VPNs increase security by requiring strong authentication of identity and encrypted data transport between the nodes for data privacy and dependability. The following sections contain information about supported transports and authentication methods.

Transport Protocols

There are two encrypted transport protocols: Layer Two Tunneling Protocol, Secure Internet Protocol (L2TP/IPSec) and Point-to-Point Tunneling Protocol (PPTP). You can enable either or both of these protocols. Each has its own strengths and requirements.

L2TP/IPSec

L2TP/IPSec uses strong IPSec encryption to tunnel data to and from network nodes. It is based on Cisco's L2F protocol.

IPSec requires security certificates (self-signed or signed by a CA such as Verisign) or a predefined shared secret between connecting nodes.

The shared secret must be entered on the server and the client.

The shared secret is not a password for authentication, nor does it generate encryption keys to establish secure tunnels between nodes. It is a token that the key management systems use to trust each other.

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

PPTP

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

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

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

Configuring L2TP/IPSec Settings

Use Server Admin to designate L2TP as the transport protocol. If you enable this protocol, you must also configure connection settings. You must designate an IPSec shared secret (if you don't use a signed security certificate), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed). If you use L2TP and PPTP, provide each protocol with a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the "any" address group, enable GRE, ESP, VPN L2TP (port 1701), and VPN ISAKMP/IKE (port 500).
- For the "192.168-net" address group, choose to allow all traffic.

To configure L2TP settings:

1 Open Server Admin and connect to the server.

2 Click the triangle at the left of the server.

The list of servers appears.

3 From the expanded Servers list, select VPN.

4 Click Settings, then click L2TP.

5 Select the "Enable L2TP over IPSec" checkbox.

6 In the "Starting IP address" field, set the beginning IP address of the VPN allocation range.

It can't overlap the DHCP allocation range, so enter 192.168.0.128.

7 In the "Ending IP address" field, set the ending IP address of the VPN allocation range.

It can't overlap the DHCP allocation range, so enter 192.168.0.255.

8 (Optional) To load-balance the VPN, select the Enable Load Balancing checkbox and enter an IP address in the Cluster IP address field.

9 Choose a PPP authentication type.

If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

If you choose RADIUS, enter the following information:

Primary IP Address: Enter the IP address of the primary RADIUS server.

Shared Secret: Enter a shared secret for the primary RADIUS server.

Secondary IP Address: Enter the IP address of the secondary RADIUS server.

Shared Secret: Enter a shared secret for the secondary RADIUS server.

- 10 In the IPSec Authentication section, enter the shared secret or select the certificate to use.

The shared secret is a common password that authenticates members of the cluster. IPSec uses the shared secret as a preshared key to establish secure tunnels between cluster nodes.

- 11 Click Save.

Configuring PPTP Settings

Use Server Admin to designate PPTP as the transport protocol.

If you enable this protocol, you must also configure connection settings. You should designate an encryption key length (40-bit or 128-bit), the IP address allocation range to be given to your clients, and the group that will use the VPN service (if needed).

If you use L2TP and PPTP, provide the protocols with a separate, nonoverlapping address range.

When configuring VPN, make sure the firewall allows VPN traffic on needed ports with the following settings:

- For the “any” address group, enable GRE, ESP, VPN L2TP (port 1701), and IKE (port 500).
- For the “192.168-net” address group, choose to allow all traffic.

To configure PPTP settings:

- 1 Open Server Admin and connect to the server.

- 2 Click the triangle at the left of the server.

The list of servers appears.

- 3 From the expanded Servers list, select VPN.

- 4 Click Settings, then click PPTP.

- 5 Select “Enable PPTP.”

- 6 If needed, select “Allow 40-bit encryption keys in addition to 128-bit” to permit 40-bit and 128-bit key encryption access to VPN.

WARNING: 40-bit encryption keys are much less secure but can be necessary for some VPN client applications.

- 7 In the “Starting IP address” field, set the beginning IP address of the VPN allocation range.

It can’t overlap the DHCP allocation range, so enter 192.168.0.128.

- 8 In the “Ending IP address” field, set the ending IP address of the VPN allocation range. It can’t overlap the DHCP allocation range, so enter 192.168.0.255.
- 9 Choose a PPP authentication type.

If you choose Directory Service and your computer is bound to a Kerberos authentication server, from the Authentication pop-up menu select Kerberos. Otherwise, choose MS-CHAPv2.

If you choose RADIUS, enter the following information:

Primary IP Address: Enter the IP address of the primary RADIUS server.

Shared Secret: Enter a shared secret for the primary RADIUS server.

Secondary IP Address: Enter the IP address of the secondary RADIUS server.

Shared Secret: Enter a shared secret for the secondary RADIUS server.
- 10 Click Save.

VPN Authentication Method

Snow Leopard Server L2TP VPN uses Kerberos v5 or Microsoft’s Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) for authentication. Snow Leopard Server PPTP VPN uses MS-CHAPv2 for authentication.

Kerberos is a secure authentication protocol that uses a Kerberos Key Distribution Server as a trusted third party to authenticate a client to a server.

MS-CHAPv2 authentication encodes passwords when they’re sent over the network, and stores them in a scrambled form on the server. This method offers good security during network transmission. It is also the standard Windows authentication scheme for VPN.

Snow Leopard Server PPTP VPN can also use other authentication methods. Each method has its own strengths and requirements. These other authentication methods for PPTP are not available in Server Admin.

To use an alternative authentication scheme (for example, to use RSA Security’s SecurID authentication), you must edit the VPN configuration file manually. The configuration file is located at /Library/Preferences/SystemConfiguration/com.apple.RemoteAccessServers.plist.

For more information, see “Offering SecurID Authentication with VPN Service” on page 196.

Using VPN Service with Users in a Third-Party LDAP Domain

To use VPN service for users in a third-party LDAP domain (an Active Directory or Linux OpenLDAP domain), you must be able to use Kerberos authentication. If you need to use MSCHAPv2 to authenticate users, you can't offer VPN service for users in a third-party LDAP domain.

Offering SecurID Authentication with VPN Service

RSA Security provides strong authentication. It uses hardware and software tokens to verify user identity. SecurID authentication is available for L2TP and PPTP transports. For details and product offerings, see www.rsasecurity.com.

Snow Leopard Server VPN service can offer SecurID authentication, but it cannot be set up in Server Admin. You can use Server Admin to configure standard VPN services, but Server Admin does not have an interface for choosing your authentication method.

If you must designate an authentication scheme (such as RSA Security SecurID) other than the default, change the VPN configuration manually.

For additional information, see the *RSA SecurID Ready Implementation Guide*, located on the web at rsasecurity.agora.com/rsasecured/guides/imp_pdfs/MacOSX_ACE_51.pdf.

To manually configure RSA Security SecurID authentication:

- 1 Open Terminal.
- 2 Create a folder named /var/ace on your Snow Leopard Server.

```
sudo mkdir /var/ace
```

Authenticate, if requested.
- 3 In Finder, choose Go > Go to Folder.
- 4 Type /var/ace.
- 5 Click Go.
- 6 Copy the sdconf.rec file from a SecurID server to /var/ace/.

You see a dialog indicating that the /var/ace/ folder cannot be modified. Click Authenticate to allow the copy.

- 7 Configure the VPN service (PPTP or L2TP) on your Snow Leopard Server to enable EAP-SecurID authentication for the protocols you want to use it with.

Enter the following in Terminal, replacing *protocol* with either *pptp* or *l2tp*:

```
sudo serveradmin settings
    vpn:Servers:com.apple.ppp.protocol:PPP:AuthenticatorEAPPlugins:\_
        _array_index:0 = "EAP-RSA"
sudo serveradmin settings
    vpn:Servers:com.apple.ppp.protocol:PPP:AuthenticatorProtocol:\_
        _array_index: = "EAP"
```

- 8 Complete the remainder of Snow Leopard Server VPN service configuration using the Server Admin.

Encrypting Observe and Control Network Data

Although Apple Remote Desktop (“Remote Management”) sends authentication information, keystrokes, and management commands encrypted by default, you might want additional security. You can choose to encrypt all Observe and Control traffic, at a performance cost.

Encryption is done using an SSH tunnel between participating computers. To use encryption for Observe and Control tasks, the target computers must have SSH enabled (“Remote Login” in the computer’s Sharing Preference pane). Additionally, firewalls between the participating computers must be configured to pass traffic on TCP port 22 (SSH well known port).

If you are trying to control a VNC server that is not a remote desktop, it cannot support Remote Desktop keystroke encryption. If you try to control that VNC server, you get a warning that the keystrokes aren’t encrypted, which you must acknowledge before you can control the VNC server. If you chose to encrypt all network data, then you cannot control the VNC server because Remote Desktop cannot open the necessary SSH tunnel to the VNC server.

To enable Observe and Control transport encryption:

- 1 Choose Remote Desktop > Preferences.
- 2 Click the Security button.
- 3 In the “Controlling computers” section, select “Encrypt all network data.”

Encrypting Network Data During File Copy and Package Installations

Remote Desktop can send files for Copy Items and Install Packages via encrypted transport. This option is not enabled by default, and you must enable it explicitly for each copy task, or in a global setting in Remote Desktop’s preferences. Even installer package files can be intercepted if not encrypted.

To encrypt individual file copying and package installation tasks:

- In the Copy Items task or Install Packages task configuration window of Remote Desktop, select “Encrypt network data.”

To set a default encryption preference for file copies:

- 1 In the Remote Desktop Preferences window, select the Security pane.
- 2 Select “Encrypt transfers when using Copy Items,” or “Encrypt transfers when using Install Packages” as needed.

Alternatively, you can encrypt a file archive before copying it. The encrypted archive can be intercepted, but it would be unreadable.

Use this chapter to learn how to secure Network and Host Access services.

You can tailor network and host access services in Snow Leopard Server to protect your computer and network users. Proper configuration of services is important and helps create a hardened shell protecting your network.

Snow Leopard Server includes several network and host access services that help you manage and maintain your network. This section describes recommended configurations for securing your network services.

For additional information about configuring network and host access services, see *Network Services Administration*.

Using IPv6 Protocol

Internet Protocol Version 6 (IPv6) is the Internet’s next-generation protocol designed to replace the current Internet Protocol, IP Version 4 (IPv4, or just IP).

IPv6 improves routing and network autoconfiguration. It increases the number of network addresses to over 3×10^{38} , and eliminates the need for Network Address Translation (NAT). IPv6 is expected to gradually replace IPv4 over a number of years, though the two will continue to coexist during this transition.

Snow Leopard Server’s network services are fully IPv6 capable and ready to transition to the next generation addressing, as well as being fully able to operate with IPv4.

Snow Leopard Server fully supports IPv6, which is configurable from Network preferences. Disable the IPv6 protocol if your server and clients do not require it. Disabling the protocol prevents potential vulnerabilities on your computer. For information about disabling IPv6, see “Securing Network Preferences” on page 118.

To enable IPv6:

- 1 Open Network preferences.
- 2 In the network connections services list, click the service to configure.
- 3 Click Advanced.
- 4 Click TCP/IP.
- 5 Choose Automatically from the Configure IPv6 pop-up menu.
If you choose Manually, you must know your assigned IPv6 address, your router's IP address, and a prefix length.
- 6 Click OK.
- 7 Click Apply.

From the command line:

```
# -----
# Enabling IPv6
#
# -----
# Enable IPv6.
#
# -----
sudo networksetup -setv6on [networkservice]
```

IPv6-Enabled Services

The following services in Snow Leopard Server support IPv6 addressing:

- DNS (BIND)
- Firewall
- Mail (POP/IMAP/SMTP)
- Windows (SMB/CIFS)
- Web (Apache 2)

These services support IPv6 addresses, but not in Server Admin. IPv6 addresses fail if entered in IP address fields in Server Admin. You can configure IPv6 addresses for these services with command-line tools and by editing configuration files.

A number of command-line tools installed with Snow Leopard Server support IPv6 (for example, `ping6` and `traceroute6`).

For more information about IPv6, see www.ipv6.org.

Securing DHCP Service

Snow Leopard Server includes dynamic host configuration protocol (DHCP) service software, which allows it to provide IP addresses, LDAP server information, and DNS server information to clients.

Disabling Unnecessary DHCP Services

Using DHCP is not recommended. Assigning static IP addresses eases accountability and mitigates the risks posed by a rogue DHCP server. If DHCP use is necessary, only one system should act as the DHCP server and the service should be disabled on all other systems.

To disable the DHCP service:

- 1 Open Server Admin and connect to the server.
- 2 Select DHCP in the Computers & Services list.
- 3 Click Stop DHCP.
- 4 Click Save.

From the command line:

```
# -----
# Securing DHCP Service
# -----  
  
# Disable DHCP Service
# -----
sudo serveradmin stop dhcp
```

Configuring DHCP Services

To use a server as a DHCP server, configure the DHCP service in Server Admin to *not* distribute DNS, LDAP, and WINS information. This is a security measure meant to protect client systems.

When client systems accept dynamically assigned DNS, LDAP, and WINS addresses, they become vulnerable to certain forms of network based attacks from rogue DHCP servers. Users may unknowingly be redirected to malicious web sites or servers.

To configure the DHCP service:

- 1 Open Server Admin and connect to the server.
- 2 Select DHCP in the Computers & Services list.
- 3 Select Subnets.
- 4 Select a subnet.
- 5 Click DNS.

- 6** Delete any name servers listed.
- 7** Click LDAP.
- 8** Delete any server information that appears.
- 9** Click WINS.
- 10** Delete the WINS information.
- 11** Click Save.

From the command line:

```
# Configuring DHCP Services
# -----
# Set a DHCP subnet's DNS, LDAP, and WINS parameters to no value
sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:dhcp_domain_name_serv
    er:_array_index:0 = ""
sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:dhcp_ldap_url:_array_
    index:0 = -empty_array
sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:WINS_node_type =" NOT
    SET"
```

Assigning Static IP Addresses Using DHCP

You can use Server Admin to assign IP addresses to specific computers. This helps simplify configuration when using DHCP and lets you have some static servers or services.

To avoid potential address conflicts and prevent hackers from easily obtaining valid IP addresses, use a static map to track network activity. A static map consists of a specific IP address assigned to a network device.

To assign a static IP address to a device, you need the device's Ethernet address (sometimes called its MAC address or hardware address). Each network interface has its own Ethernet address.

If you have a computer that moves between wired and wireless networks, it uses two Ethernet addresses: one for the wired connection, and one for the wireless connection.

To assign a static IP address:

- 1** Open Server Admin and connect to the server.
- 2** Select DHCP in the Computers & Services list.
- 3** Click Static Maps.
- 4** Click Add Computer.

- 5** Enter the name of the computer.
- 6** In the Network Interfaces list, click the column to enter the following information:
 - MAC Address of the computer that needs a static address.
 - IP address you want to assign to the computer.
- 7** If the computer has other network interfaces that require static IP addresses, click the Add (+) button and enter the IP address for each interface.
- 8** Click OK.
- 9** Click Save.

From the command line:

```
# Set a DHCP client's static IP address
#
# -----
# Each computer needs its own GUID within the static map array.
# Increment the array index value for network interfaces
# for a single computer.
serveradmin settings
    dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:ip_address:_array_i
    ndex:0 = $ASSIGNED_IP_ADDRESS
serveradmin settings
    dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:en_address:_array_i
    ndex:0 = $COMPUTER_MAC_ADDRESS
serveradmin settings
    dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:name =
    $COMPUTER_NAME
```

Securing DNS Service

Snow Leopard Server uses Berkeley Internet Name Domain (BIND) v9.4.1 for its implementation of DNS protocols. BIND is an open source implementation and is used by most name servers on the Internet.

If your server is not intended to be the authoritative DNS server for your namespace, disable the DNS service in Server Admin.

To disable the DNS service:

- 1** Open Server Admin and connect to the server.
- 2** Select DNS in the Computers & Services list.
- 3** Click Stop DNS.
- 4** Click Save.

From the command line:

```
# -----
# Securing DNS Service
# -----

# Disable DNS Service.
# -----
sudo serveradmin stop dns
```

Understanding BIND

BIND is the set of programs used by Snow Leopard Server that implements DNS. One of those programs is the *name daemon*, or *named*. To set up and configure BIND, you must change the configuration file and the zone file. The configuration file is /etc/named.conf.

The zone file name is based on the name of the zone. For example, the zone file example.com is /var/named/example.com.zone.

If you edit named.conf to configure BIND, don't change the *inet* settings of the controls statement. Otherwise, Server Admin can't retrieve status information for DNS.

The *inet* settings should look like this

```
controls {
    inet 127.0.0.1 port 54 allow {any;};
    keys { "rndc-key"; };
};
```

Using Server Admin after editing BIND configuration files might overwrite changes.

For more information about DNS and BIND, see the following:

- *DNS and BIND, 5th edition*, by Paul Albitz and Cricket Liu (O'Reilly and Associates, 2006)
- The International Software Consortium website:www.isc.org and www.isc.org/sw/bind
- The DNS Resources Directory:www.dns.net/dnsrd

Turning Off Zone Transfers

Unless your site requires them, use Server Admin to turn off zone transfers and recursive DNS queries.

To turn off zone transfers and recursive DNS queries:

- 1 Open Server Admin and connect to the server.
- 2 Select DNS in the Computers & Services list.

- 3** Click Zones.
- 4** Select the primary zone you want to change.
- 5** Click General.
- 6** Deselect “Allows zone transfer” to prevent hosts on the network from getting copies of the primary zone data.
If needed, set up zone transfers so they only occur between trusted servers. This requires manually editing the BIND configuration files.
- 7** Click Save.

Disabling Recursion

Recursion fully resolves domain names into IP addresses. Applications depend on the DNS server to perform this function. Other DNS servers that query your DNS servers don’t need to perform the recursion.

To prevent malicious users from changing the primary zone’s records (referred to as cache poisoning) and to prevent unauthorized use of the server for DNS service, you can restrict recursion using Server Admin. However, if you prevent your private network from using recursion, users can’t use your DNS service to look up names outside of your zones.

Disable recursion only if no clients are using this DNS server for name resolution and no servers are using it for forwarding.

If your site requires recursion, allow recursive queries only from trusted clients and not from external networks.

If you enable recursion, consider disabling it for external IP addresses but enabling it for internal IP addresses. This requires manually editing the BIND configuration files.

To disable recursion:

- 1** Open Server Admin and connect to the server.
- 2** Select DNS in the Computers & Services list.
- 3** Click Settings.
- 4** Remove all entries except “localhost” from the “Accept recursive queries from the following networks” list using the Remove (–) button.
- 5** Click Save.

Make sure that forward and reverse zones are established and fully populated. Otherwise, any Open Directory server using the DNS service will not work correctly.

Preventing Some DNS Attacks

DNS servers are targeted by malicious computer users (hackers). DNS servers are susceptible to several kinds of attacks. By taking extra precautions, you can prevent the problems and downtime associated with hackers.

Several kinds of security attacks are associated with DNS service:

- DNS cache poisoning
- Server mining
- DNS service profiling
- Denial of service (DoS)
- Service piggybacking

DNS Cache Poisoning

DNS cache poisoning (a form of DNS spoofing) is the adding of false data to the DNS server's cache. This enables hackers to:

- Redirect real domain name queries to alternative IP addresses.

For example, a falsified A record for a bank could point a computer user's browser to a different IP address that is controlled by the hacker. A duplicate website could fool users into giving their bank account numbers and passwords to the hacker.

Also, a falsified mail record could enable a hacker to intercept mail sent to or from a domain. If the hacker then forwards that mail to the correct mail server after copying the mail, this can go undetected.

- Prevent proper domain name resolution and access to the Internet.

This is the most benign of DNS cache poisoning attacks. It makes a DNS server appear to be malfunctioning.

The most effective method to prevent these attacks is vigilance. This includes maintaining up-to-date software.

If exploits are found in the current version of BIND, the exploits are patched and a security update is made available for Snow Leopard Server. Apply all such security patches.

Server Mining

Server mining is the practice of getting a copy of a complete primary zone by requesting a zone transfer. In this case, a hacker pretends to be a secondary zone to another primary zone and requests a copy of the primary zone's records.

With a copy of your primary zone, the hacker can see what kinds of services a domain offers and the IP addresses of the servers that offer them. He or she can then try specific attacks based on those services. This is reconnaissance before another attack.

To prevent this attack, disable zone transfers. If required, specify which IP addresses have permission to request zone transfers (your secondary zone servers) and deny all others.

Zone transfers are accomplished over TCP on port 53. To limit zone transfers, block zone transfer requests from anyone but your secondary DNS servers.

To specify zone transfer IP addresses:

- 1 Create a firewall filter that permits only IP addresses that are inside your firewall to access TCP port 53.
- 2 Follow the instructions in “Creating Advanced Firewall Rules” on page 217 using the following settings:
 - Packet: Allow
 - Port: 53
 - Protocol: TCP
 - Source IP: the IP address of your secondary DNS server
 - Destination IP: the IP address of your primary DNS server

DNS Service Profiling

Another common reconnaissance technique used by malicious users is to profile your DNS service. First a hacker makes a BIND version request. The server reports what version of BIND is running. Then the hacker compares the response to known exploits and vulnerabilities for that version of BIND.

To prevent this attack, configure BIND to respond with something other than what it is.

To alter BIND’s version response:

- 1 Open a command-line text editor (for example `vi`, `emacs`, or `pico`).
- 2 Open `named.conf` for editing.
- 3 To the options brackets of the configuration file, add the following:

```
version      "[your text, maybe 'we're not telling!']";
```
- 4 Save `named.conf`.

Denial of Service (DoS)

This kind of attack is common and easy. A hacker sends so many service requests and queries that a server uses all its processing power and network bandwidth trying to respond. The hacker prevents legitimate use of the service by overloading it.

It is difficult to prevent this type of attack before it begins. Constant monitoring of the DNS service and server load enables an administrator to catch the attack early and mitigate its damaging effect.

The easiest way to prevent this attack is to block the offending IP address with your firewall. Unfortunately, this means the attack is already underway and the hacker's queries are being answered and the activity logged.

Service Piggybacking

This attack is done not so much by malicious intruders but by common Internet users who learn the trick from other users. They might feel that the DNS response time with their own ISP is too slow, so they configure their computer to query another DNS server instead of their own ISP's DNS servers. Effectively, there are more users accessing the DNS server than were planned for.

You can prevent this type of attack by limiting or disabling DNS recursion. If you plan to offer DNS service to your LAN users, they need recursion to resolve domain names, but don't provide this service to Internet users.

To prevent recursion entirely, see "Disabling Recursion" on page 204.

The most common balance is permitting recursion for requests coming from IP addresses in your own range but denying recursion to external addresses.

ARP Spoofing

This type of attack, also known as ARP poisoning, allows an attacker to take over a computer's IP address by manipulating the ARP caches of other hosts on the network. The attacker must be on the same network as the computer it is attacking or the host that the computer is communicating with.

The attacker can also use ARP spoofing for a man-in-the-middle attack, which forwards traffic from a computer to the attacker's computer. This allows the attacker to view packets and look for passwords and confidential data. ARP spoofing can also be used to create a DoS attack, stopping all network traffic.

By configuring your network with static IP addresses and monitoring your network traffic, you can keep unauthorized users from maliciously using your network.

Securing NAT Service

NAT is a protocol you use to give multiple computers access to the Internet using only one assigned public or external IP address. NAT permits you to create a private network that accesses the Internet through a NAT router or gateway. NAT is sometimes referred to as IP masquerading.

The NAT service further enhances security by limiting communication between your private network and a public network (such as the Internet):

- Communication from a computer on your private network is translated from a private IP address to a shared public IP address. Multiple private IP addresses are configured to use a single public IP address.

- Communication to your private network is translated and forwarded to an internal private IP address (IP forwarding). The external computer cannot determine the private IP address. This creates a barrier between your private network and the public network.
- Communication from a public network cannot come into your private network unless it is requested. It is only allowed in response to internal communication.

Note: If using NAT, consider combining NAT routing with other network services.

The NAT router takes all traffic from your private network and remembers internal addresses that have made requests. When the NAT router receives a response to a request, it forwards it to the originating computer. Traffic that originates from the Internet does not reach computers behind the NAT router unless port forwarding is enabled.

Important: Firewall service must be enabled for NAT to function.

If your server is not intended to be a NAT server, deactivate the NAT server software.

To disable NAT service:

- 1 Open Server Admin and connect to the server.
- 2 Select NAT in the Computers & Services list.
- 3 Click Stop NAT.
- 4 Click Save.

From the command line:

```
# -----
# Securing NAT Service
# -----  
  
# Disable NAT service.
# -----
sudo serveradmin stop nat
```

Configuring Port Forwarding

You can direct traffic coming in to your NAT network to a specific IP address behind the NAT gateway. This is called *port forwarding*.

Port forwarding can be used to route external-facing uncommon open ports on the firewall to common internal ports, obscuring what services are active through the NAT barrier. This practice is not reliable and should not be solely depended on to hide active services on the computer.

Port forwarding lets you set up computers on the internal network that handle incoming connections without exposing other computers to outside connections. For example, you could set up a web server behind the NAT service and forward incoming TCP connection requests on port 80 to the designated web server.

You can't forward the same port to multiple computers, but you can forward many ports to one computer. Enabling port forwarding requires the use of the Terminal application and administrator access to root privileges through `sudo`.

You must also create a plist file. The contents of the plist file are used to generate `/etc/nat/natd.conf.apple`, which is passed to the NAT daemon when it is started.

Do not try to edit `/etc/nat/natd.conf.apple` directly. If you use a plist editor instead of a command-line text editor, alter the following procedure to suit.

To configure port forwarding:

- 1 If the file `/etc/nat/natd.plist` doesn't exist, make a copy of the default NAT daemon plist.

```
sudo cp /etc/nat/natd.plist.default /etc/nat/natd.plist
```

- 2 Using a Terminal editor, add the following block of XML text to `/etc/nat/natd.plist` before the two lines at the end of the file (`</dict>` and `</plist>`), substituting your settings where indicated by *italics*:

```
<key>redirect_port</key>
<array>
<dict>
<key>proto</key>
<string>tcp or udp</string>
<key>targetIP</key>
<string>LAN_ip</string>
<key>targetPortRange</key>
<string>LAN_ip_range</string>
<key>aliasIP</key>
<string>WAN_ip</string>
<key>aliasPortRange</key>
<string>WAN_port_range</string>
</dict>
</array>
```

- 3 Save your file changes.
- 4 Enter the following commands in the Terminal:
`sudo serveradmin stop nat`
`sudo serveradmin start nat`
- 5 Verify that your changes remain by inspecting the `/etc/nat/natd.conf.apple` file.

The changes made, except for comments and those settings that Server Admin can change, are used by server configuration tools (Server Admin, Gateway Setup Assistant, and sudo serveradmin).

- 6 Click Save.
- 7 Start NAT service.

Disabling NAT Port Mapping Protocol

NAT Port Mapping Protocol (NAT-PMP) allows a computer behind the NAT router to automatically configure the router to allow computers outside the private network to contact itself. NAT-PMP automates the process of port forwarding, allowing the internal network computers control the forwarding.

If you do not want your internal clients to change port-forwarding rules disable NAT-PMP.

To configure NAT service:

- 1 Open Server Admin and connect to the server.
- 2 Select NAT in the Computers & Services list.
- 3 Click Settings.
- 4 Deselect “Enable NAT Port Mapping Protocol.”
- 5 Click Save.

Securing Bonjour (mDNS)

Bonjour is a protocol for discovering file, print, chat, music sharing, and other services on IP networks. Bonjour listens for service inquiries from other computers and provides information about available services. Users and applications on your local network can use Bonjour to quickly determine which services are available on your computer, and you can use it to determine which services are available on theirs.

This easy exchange of information makes service discovery very convenient, but it also incurs a security risk. Bonjour broadcasts the services that are present and the services you have available. These risks must be weighed against the utility of running a network service such as Bonjour.

Aside from the information freely exchanged by Bonjour, network services inherently incur a security risk due to the potential for implementation errors to allow remote attackers to access your system. However, Bonjour mitigates these risks by implementing sandboxing.

To reduce the security risk of running Bonjour, connect only to secure, trusted local networks. Also verify that Network preferences enables only required networking connections. This reduces the chance of connecting to an insecure network.

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

If you cannot trust all services on your local network, then Bonjour should not be used.

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

To disable Bonjour advertising, enter the following commands:

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

For example:

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

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

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

For example:

```
<key>ProgramArguments</key>
```

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

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

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

You must also block Bonjour from listening for and accepting Bonjour traffic by creating a firewall rule using ipfw. This prevents your computer from receiving potentially malicious Bonjour traffic from the network. If you haven't set up IPFW to run when the computer starts up, see Chapter 13, "Configuring the Firewall."

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

To block Bonjour listening:

```
# Block Bonjour listening.  
# -----  
# Default Setting.  
# Bonjour is enabled  
# Firewall is disabled  
  
# Suggested Setting.  
# Add the following line to /etc/ipfw.conf.  
add 00001 deny udp from any to me dst-port 5353  
# Reload the firewall rules.  
sudo /sbin/ipfw flush  
sudo /sbin/ipfw /etc/ipfw.conf
```

If Bonjour is disabled, you must manually configure network printers. Disabling Bonjour can also disable functionality in other applications that rely on Bonjour or possibly make them unusable.

If disabling Bonjour interferes with other applications that are needed by the user, remove the <string>-NoMulticastAdvertisements</string> from the mDNSResponder.plist file. Then unblock UDP port 5353 on your firewall.

Configuring the Firewall

Use this chapter to learn how configure the IPFW2 firewall.

Using a firewall to filter network traffic from a host or a network of hosts prevents attackers from gaining access to your computer.

About Firewall Protection

Firewall service is software that protects network applications running on your Snow Leopard Server computer.

Turning on firewall service is similar to installing a filter to limit access to your network. firewall service scans incoming IP packets and rejects or accepts these packets based on rules you use to configure firewall service.

You can monitor activity involving your firewall by enabling firewall logging. Firewall logging creates a log file that tracks activity such as the sources and connection attempts blocked by the firewall. You can view this log in the Console utility.

You can restrict access to any IP service running on the server, and you can customize rules for incoming clients or for a range of client IP addresses.

Important: Firewall service can disrupt network communications and its configuration can be complicated to implement. Do not implement recommendations without understanding their purpose or impact.

Services such as Web and FTP services are identified on your server by a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number. When a computer tries to connect to a service, firewall service scans the rule list for a matching port number.

When running, the default firewall configuration on Snow Leopard Server denies access to incoming packets from remote computers except through ports for remote configuration. This provides a high level of security.

Stateful rules are in place as well, so responses to outgoing queries initiated by your computer are also permitted. You can then add rules to permit server access to those clients who require access to services.

Important: You should not perform any firewall configuration remotely because of the risk of disabling communications to the remote host.

Planning Firewall Setup

Plan your firewall service by deciding which services you want to provide access to. Mail, Web, and FTP services generally require access by computers on the Internet. File and Print services are most likely restricted to your local subnet.

After you decide which services to protect using firewall service, determine which IP addresses you want to access your server. Then create the appropriate rules.

After the firewall service is configured, network users might request that the rules be changed to allow additional services. These changes should be resisted and an approval process should be put in place to monitor these changes.

Configuring the Firewall Using Server Admin

Advanced configuration servers use ipfw2 for firewall service. The application-level firewall is available only to standard and workgroup configuration installations.

Starting Firewall Service

By default, firewall service blocks incoming TCP connections and denies UDP packets, except those received in response to outgoing requests from the server.

Before you turn on firewall service, make sure you've set up rules permitting access from IP addresses you choose; otherwise, no one can access your server.

If you add or change a rule after starting firewall service, the new rule affects connections already established with the server. For example, if you deny all access to your FTP server after starting firewall service, computers connected to your FTP server are disconnected.

To start firewall service:

- 1 Open Server Admin and connect to the server.
- 2 Select Firewall in the Computers & Services list.
- 3 Click the Start Firewall button below the Servers list.

From the command line:

```
# -----
# Securing Firewall Service
# -----

# Start firewall service.
# -----
sudo serveradmin start ipfilter
```

Creating an IP Address Group

By grouping IP addresses you can simultaneously set firewall rules for large numbers of network devices and allow for much better organization. This enhances the security of your network.

These groups are used to organize and target the rules. The “any” address group is for all addresses. Two other IP address groups are present by default, intended for the entire “10.0.0.0” range of private addresses and the entire “192.168.0.0” range of private addresses.

Addresses can be listed as individual addresses (192.168.2.2), IP address and CIDR notation (192.168.2.0/24), or IP address and netmask notation (192.168.2.0:255.255.255.0).

By default, an IP address group is created for all incoming IP addresses. Rules applied to this group affect all incoming network traffic.

To create an address group:

- 1 Open Server Admin and connect to the server.
- 2 Select Firewall in the Computers & Services list.
- 3 Click Settings, then click Address Groups.
- 4 Below the IP Address Groups list, click the Add (+) button.
- 5 In the Group name field, enter a group name.
- 6 Enter the addresses and subnet mask you want the rules to affect.
Use the Add (+) and Delete (-) buttons.
To indicate any IP address, use the word “any.”
- 7 Click OK.
- 8 Click Save.

Creating Firewall Service Rules

By default, firewall service permits all UDP connections and blocks incoming TCP connections on ports that are not essential for remote administration of the server. Also, by default, stateful rules are in place that permit specific responses to outgoing requests.

Before you turn on firewall service, make sure you've set up rules permitting access from IP addresses you choose; otherwise, no one can access your server.

You can easily permit standard services through the firewall without advanced and extensive configuration. Standard services include:

- SSH access
- Web service
- Apple File service
- Windows File service
- FTP service
- Printer Sharing
- DNS/Multicast DNS
- ICMP Echo Reply (incoming pings)
- IGMP
- PPTP VPN
- L2TP VPN
- QTSS media streaming
- iTunes Music Sharing

If you add or change a rule after starting firewall service, the new rule affects connections already established with the server. For example, if you deny all access to your FTP server after starting firewall service, computers connected to your FTP server are disconnected.

To configure firewall standard services:

- 1 Open Server Admin and connect to the server.
- 2 Select Firewall in the Computers & Services list.
- 3 Click Settings, then click Services.
- 4 From the Edit Services for pop-up menu, select an address group.
- 5 For the address group, choose to permit all traffic from any port or to permit traffic on designated ports.

- 6** For each service you want the address group to use, select Allow.
If you don't see the service you need, add a port and description to the services list.
To create a custom rule, see "Creating Advanced Firewall Rules" on page 217.
- 7** Click Save.

Creating Advanced Firewall Rules

You use the Advanced Settings pane in Server Admin to configure specific rules for firewall service. Firewall rules contain originating and destination IP addresses with subnet masks. They also specify what to do with incoming network traffic. You can apply a rule to all IP addresses, a specific IP address, or a range of IP addresses.

Addresses can be listed as individual addresses (192.168.2.2), IP address and subnet mask in CIDR notation (192.168.2.0/24), or IP address and subnet mask in netmask notation (192.168.2.0:255.255.255.0).

To set up an advanced firewall rule:

- 1** Open Server Admin and connect to the server.
- 2** Select Firewall in the Computers & Services list.
- 3** Click Settings, then click Advanced.
- 4** Click the Add (+) button.
Alternatively, you can select a rule similar to the one you want to create, click Duplicate, and then click Edit.
- 5** In the Action pop-up menu, select whether this rule permits or denies access.
If you choose Other, enter the needed action (for example, log).
- 6** From the Protocol pop-up menu, choose a protocol.
If you choose Other, enter the needed protocol (for example, icmp, esp, ipencap).
- 7** From the Service pop-up menu, choose a service.
To select a nonstandard service port, choose Other.
- 8** If needed, choose to log all packets that match the rule.
- 9** For the source of filtered traffic, choose an address group from the Address pop-up menu.
If you don't want to use an existing address group, enter the source IP address range (using CIDR notation) you want to filter.
If you want it to apply to any address, choose "any" from the pop-up menu.
- 10** If you selected a nonstandard service port, enter the source port number.
- 11** For the destination of filtered traffic, choose an address group from the Source pop-up menu.

If you don't want to use an existing address group, enter the destination IP address range (using CIDR notation).

If you want it to apply to any address, choose "any" from the pop-up menu.

12 If you selected a nonstandard service port, enter the destination port number.

13 From the Interface pop-up menu that this rule will apply to, choose In or Out.

In refers to the packets being sent to the server.

Out refers to the packets being sent from the server.

14 If you select Other, enter the interface name (en0, en1, fw1, and so on).

15 Click OK.

16 Click Save to apply the rule immediately.

Enabling Stealth Mode

You can hide your firewall by choosing not to send a connection failure notification to any connection that is blocked by the firewall. This is called stealth mode and it effectively hides your server's closed ports.

For example, if a network intruder tries to connect to your server, even if the port is blocked, he or she knows that there is a server and can find other ways to intrude.

If stealth mode is enabled, instead of being rejected, the hacker won't receive notification that an attempted connection took place.

To enable stealth mode:

1 Open Server Admin and connect to the server.

2 Select Firewall in the Computers & Services list.

3 Click Settings, then click Advanced.

4 Select "Enable for TCP," "Enable for UDP," or both, as needed.

5 Click Save.

From the command line:

```
# Enable stealth mode.  
# -----  
sudo serveradmin settings ipfilter:blackHoleTCP = true  
sudo serveradmin settings ipfilter:blackHoleUDP = true
```

Viewing the Firewall Service Log

Each rule you set up in Server Admin corresponds to rules in the underlying firewall software. Log entries show you when the rule was applied, the IP address of the client and server, and other information.

The log view shows the contents of `/var/log/ipfw.log`. You can refine the view using the text filter box.

To view the firewall service log:

- 1 Open Server Admin and connect to the server.
- 2 Select Firewall in the Computers & Services list.
- 3 Click Log.

To search for specific entries, use the Filter field above the log.

From the command line:

```
# View the firewall service log.  
# -----  
sudo tail /var/log/ipfw.log
```

The filters you create in Server Admin correspond to rules in the underlying filtering software. Log entries show you the rule applied, the IP address of the client and server, and other information. For more information about rules and what they mean, see “Creating Advanced Firewall Rules” on page 217.

Here are some examples of firewall log entries and how to read them.

Log Example 1

```
Dec 12 13:08:16 ballch5 mach_kernel: ipfw: 65000 Unreach TCP  
10.221.41.33:2190 192.168.12.12:80 in via en0
```

This entry shows that firewall service used rule 65000 to deny (unreach) the remote client at 10.221.41.33:2190 from accessing server 192.168.12.12 on web port 80 through Ethernet port 0.

Log Example 2

```
Dec 12 13:20:15 mayalu6 mach_kernel: ipfw: 100 Accept TCP 10.221.41.33:721  
192.168.12.12:515 in via en0
```

This entry shows that firewall service used rule 100 to permit the remote client at 10.221.41.33:721 to access the server 192.168.12.12 on the LPR printing port 515 through Ethernet port 0.

Log Example 3

```
Dec 12 13:33:15 smithy2 mach_kernel: ipfw: 10 Accept TCP 192.168.12.12:49152  
192.168.12.12:660 out via lo0
```

This entry shows the NAT divert rule applied to an outbound packet. In this case it diverts the rule to service port 660, which is the port the NAT daemon uses.

Configuring the Firewall Manually

The IPFW2 firewall (also referred to here as IPFW) allows for the creation of complex and powerful packet filtering rulesets. This firewall can be difficult to configure, and can also disrupt network communications if improperly configured. It requires manually written rules, and the system must be configured to read those rules at startup.

Configuring IPFW rulesets requires a higher level of expertise than many system administration tasks. If an administrator is not mindful of the IPFW ruleset on the system, confusion can arise when some network connectivity is not available that should be.

Understanding IPFW Rulesets

An IPFW configuration or ruleset is a list of rules that are designed to match packets and take appropriate action. IPFW rules are numbered from 1 to 65535. The packet passed to the firewall is compared against each of the rules (in numerical order). When the packet matches a rule, the corresponding action is taken.

A more complete description of the capabilities and configuration of IPFW can be found in the `ipfw` man page.

The IPFW ruleset can be stored as a list of IPFW rules inside a text file. Traditionally, the file `/etc/ipfw.conf` is used to store these rules.

To view enforced IPFW rules, run the command:

```
sudo ipfw print
```

The default output should appear something like this:

```
65535 allow ip from any to any
```

This line shows that the default configuration allows all traffic through the IPFW firewall, performing no filtering. Like all IPFW rules, it consists of a rule number (65535); an action (allow); and body (ip from any to any).

In this case, the body (ip from any to any) matches all IP packets. This also happens to be a special rule, called the default rule. It is the highest-numbered rule possible and is compiled directly into the kernel.

Because no rules have actually been added to the system, all packets are passed to this default rule, which allows them all through. However, if the Stealth Mode feature is enabled on the system, then the following line appears first in the list:

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

This rule shows the implementation of Stealth Mode, dropping incoming ping echo requests, which is ICMP type 8. Because it is a lower rule number (and thus appears earlier when listed), it is consulted before the default rule.

Use this chapter to learn how to secure collaboration services.

Collaboration services help users share information for increased productivity. Securing the access and transfer of shared information protects your data.

Collaboration services promote interactions among users, facilitating teamwork and productivity. This chapter describes how to secure iCal, iChat, Wiki, and Podcast Producer collaboration services.

For information about configuring collaboration services, see *iCal Server Administration*, *iChat Service Administration*, *Web Technologies Administration*, and *Podcast Producer Administration*.

Securing iCal Service

Security for iCal service consists of two main areas:

- **Securing the authentication:** This means using a method of authenticating users that is secure and doesn't pass login credentials in clear text over the network. The high-security authentication used pervasively in Snow Leopard Server is Kerberos v5. To learn how to configure secure authentication, see "Choosing and Enabling Secure Authentication for iCal Service" on page 223.
- **Securing the data transport:** This means encrypting the network traffic between the calendar client and the calendar server. When the transport is encrypted, no one can analyze the network traffic and reconstruct the contents of the calendar. iCal service uses SSL to encrypt the data transport.
To learn how to configure and enable SSL for iCal service, see "Configuring and Enabling Secure Network Traffic for iCal Service" on page 224.

Disabling iCal Service

If your server is not intended to be an iCal server, disable the iCal server software. Disabling the service prevents potential vulnerabilities on your computer.

To disable iCal service:

- 1 Open Server Admin and connect to the server.
- 2 Select iCal in the Computers & Services list.
- 3 Click Stop iCal.

From the command line:

```
# -----
# Securing Collaboration Services
# -----



# -----
# Securing iCal service
# -----



# Disable iCal service.
# -----
sudo serveradmin stop calendar
```

Securely Configuring iCal Service

To securely configure iCal service, you must secure authentication and data transport.

Choosing and Enabling Secure Authentication for iCal Service

Users authenticate to iCal service through one of the following methods:

- **Kerberos v5:** This method uses strong encryption and is used in Snow Leopard for single sign-on to services offered by Snow Leopard Server.
- **Digest:** (RFC 2617) This method sends secure login names and encrypted passwords without the use of a trusted third-party (like the Kerberos realm), and is usable without maintaining a Kerberos infrastructure.
- **Any:** This method includes Kerberos v5 and Digest authentication. The client can choose the most relevant method for what it can support.

You can set the required authentication method using Server Admin. To enable the highest security, choose a method other than "Any."

To choose an authentication method:

- 1 In Server Admin, select a server and choose the iCal service.
- 2 Click the Settings button in the toolbar.
- 3 Select the method from the Authentication pop-up menu.

- 4 Click Save, then restart the service.

From the command line:

```
# Choose an authentication method for iCal service.  
# -----  
# To enable all auth methods:  
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"  
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "yes"  
sudo serveradmin stop calendar; sudo serveradmin start calendar  
  
# To choose Digest auth only:  
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "no"  
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "yes"  
sudo serveradmin stop calendar; sudo serveradmin start calendar  
  
# For Kerberos only:  
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"  
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "no"  
sudo serveradmin stop calendar; sudo serveradmin start calendar
```

Configuring and Enabling Secure Network Traffic for iCal Service

When you enable Secure Sockets Layer (SSL), you encrypt all data sent between the iCal server and the client. To enable SSL, you must select a certificate. If you use the default self-signed certificate, the clients must choose to trust the certificate before they can make a secure connection.

To enable secure network traffic using SSL transport:

- 1 In Server Admin, select a server and choose the iCal service.
- 2 Click the Settings button in the toolbar.
- 3 Click Enable Secure Sockets Layer (SSL).
- 4 Choose a TCP port for SSL to communicate on.
The default port is 8443.
- 5 Choose the certificate to be used for encryption.
- 6 Click Save, then restart the service.

From the command line:

```
# Enable secure network traffic using SSL transport.  
# -----  
sudo serveradmin settings calendar:SSLPort = 8443
```

Viewing iCal Service Logs

iCal service logging is important for security. With logs, you can monitor and track communication through the iCal service. You can access the iCal service log, /var/log/system.log using Server Admin.

To view the iCal service log:

- 1 Open Server Admin and connect to the server.
 - 2 Click the triangle at the left of the server.
- The list of services appears.
- 3 Click iCal.
 - 4 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
# View the iCal service log  
# -----  
sudo tail /var/log/caldavd/access.log
```

Securing iChat Service

The iChat service provides a secure way for users to chat. To use iChat service on a server, users must be defined in directories the server uses to authenticate users. For more information about configuring search paths to directories, see the *Open Directory Administration*.

Disabling iChat Service

If your server is not intended to be an iChat server, disable the iChat server software. Disabling the software prevents potential vulnerabilities on your computer.

To disable iChat service:

- 1 Open Server Admin and connect to the server.
- 2 Select iChat in the Computers & Services list.
- 3 Click Stop iChat.

From the command line:

```
# Disable iChat service.  
# -----  
sudo serveradmin stop jabber
```

Securely Configuring iChat Service

If your organization requires the use of iChat service, configure it to use SSL. SSL communication certifies the identity of the server and establishes secure, encrypted data exchange.

You identify an SSL certificate for iChat service to use the first time you set up iChat service, but you can use a different certificate later. You can use a self-signed certificate or a certificate imported from a CA. For more information about defining, obtaining, and installing certificates on your server, see “Readyng Certificates” on page 168.

Sending messages to multiple recipients over an internal iChat sever does not require a MobileMe identity. The internal iChat server (*jabberd*) requires a server-side SSL certificate that is used by each client to establish an SSL session (similar to a web access session). A MobileMe certificate is required to establish encrypted sessions between two iChat clients communicating using text, audio, and video.

To securely configure iChat service:

- 1 Open Server Admin and connect to the server.
- 2 Select iChat in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 Click the Add (+) button to add host domains.

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

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

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

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

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

- 6 Choose the method of authentication from the Authentication pop-up menu:

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

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

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

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

- 8 If you are using a certificate with iChat, select “Require secure server-to-server federation.”

This option requires an SSL certificate to be installed, which is used to secure the server-to-server federation.

- 9 To restrict server-to-server communication to servers that are listed, select “Allow federation with the following domains.”

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

- 10 Click Save, and then click Start Service.

- 11 Make sure the iChat server’s Open Directory search path includes directories where users and group members that you want to communicate using iChat service are defined.

The *Open Directory Administration Guide* explains how to set up search paths.

Any user or group member defined in the Open Directory search path is now authorized to use iChat service on the server, unless you deny them access to iChat service.

From the command line:

```
# Securely configure iChat service.  
# To select an iChat server certificate:  
sudo serveradmin settings jabber:sslKeyFile = "/etc/certificates/  
Default.crtkey"  
  
# (Or replace the path with the full path to the certificate that you want  
# to select.)  
# Restart the service if it is running:  
sudo serveradmin stop jabber; sudo serveradmin start jabber  
  
# To select an iChat server auth method use one of the following:  
sudo serveradmin settings jabber:authLevel = "ANYMETHOD"  
sudo serveradmin settings jabber:authLevel = "KERBEROS"  
sudo serveradmin settings jabber:authLevel = "STANDARD"  
  
# Then restart the service:  
sudo serveradmin stop jabber  
sudo serveradmin start jabber
```

Using Certificates to Secure S2S Communication

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

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

Jabber provides the following ports:

- 5222 accepts TLS encryption
- 5223 accepts SSL encryption

SSL encrypts your chat message over the network between client-to-server and server-to-server connections. However, if your iChat server is logging chat messages, your messages are stored in a unencrypted format that can be easily viewed by your server administrator.

To select a certificate:

- 1 Open Server Admin and connect to the server.
- 2 Select iChat in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 From the SSL Certificate pop-up menu, choose an SSL certificate.
The menu lists all SSL certificates that are installed on the server.
To create or add certificates, choose Manage Certificates from the SSL Certificate pop-up menu.
- 5 Click Save.

From the command line:

```
#  
# Select a certificate.  
# -----  
sudo serveradmin settings jabber:sslKeyFile = "/etc/certificates/  
Default.crtkey"
```

Additional Security Enhancements

For additional security enhancements, you can further restrict the iChat service by using SACLs and firewall rules. These are configured based on your organization’s network environment.

You can configure SACLs to restrict iChat access to specific users or groups. For more information about configuring SACLs, see “Setting Service Access Control Lists (SACLs)” on page 183.

You can configure firewall rules that prevent iChat connections from unintended sources. For more information, see “Creating Firewall Service Rules” on page 216.

Viewing iChat Service Logs

iChat service logging is important for security. With logs, you can monitor and track communication through the iChat service. Access the iChat service log, /var/log/system.log, using Server Admin.

To view the iChat service log:

- 1 Open Server Admin and connect to the server.
 - 2 Click the triangle at the left of the server.
- The list of services appears.
- 3 Click iChat.
 - 4 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
# View the iChat service log.  
# -----  
sudo tail /var/log/server.log | grep jabberd
```

Securing Wiki Service

The level of website security determines the level of wiki security. Wiki security is established when the website that the wiki is configured on is secure.

Disabling Wiki Service

If your server does not provide wiki service, disable the wiki portion of the web service software. Disabling wiki service does not prevent potential vulnerabilities with other web sites hosted on the server.

To disable wiki service:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites.
- 4 Select the web site that hosts the wiki.
- 5 Click Web Services.
- 6 Deselect Wikis.

From the command line:

```
# -----  
# Securing Wiki Service  
# -----  
  
# Disable Wiki service.  
# -----  
sudo serveradmin stop teams
```

Securely Configuring Wiki Services

Methods you can use to help secure data moving to and from your wiki include the following:

- Set up SSL for the website your wiki is running on. SSL provides security for a site and its users by authenticating the server, encrypting information, and maintaining message integrity. For more information, see “Enabling Secure Sockets Layer (SSL)” on page 276.
- Restrict users and groups that can create wiki pages on your website by adding users and groups to the web services list. For more information, see “Securing Web Service” on page 271.

Viewing Wiki Service Logs

Wiki service logging is important for security. With logs, you can monitor and track communication through the wiki service. Access the wiki service logs, /Library/Logs/wikid/error.log and /Library/Logs/wikid/access.log, using Server Admin.

To view the wiki service log:

- 1 Open Server Admin and connect to the server.
 - 2 Click the triangle at the left of the server.
- The list of services appears.
- 3 Click Wiki.
 - 4 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
#  
# View the wiki service log.  
# -----  
sudo tail /Library/Logs/wikid/access.log
```

Securing Podcast Producer Service

To secure Podcast Producer service, disable it if you don't use it. If you use the service, use Server Admin to control access to workflows and cameras.

Disabling Podcast Producer Service

If your server is not a Podcast Producer server, disable the Podcast Producer server software. Disabling the software prevents potential vulnerabilities on your computer.

To disable Podcast Producer service:

- 1 Open Server Admin and connect to the server.
- 2 Select Podcast Producer in the Computers & Services list.
- 3 Click Stop Podcast Producer.

From the command line:

```
# -----
# Securing Podcast Producer Service
# -----  
  
# Disable Podcast Producer service.
# -----
sudo serveradmin stop pcast
```

Securely Configuring Podcast Producer Service

To protect the Podcast Producer service from being exploited, control access to workflows and cameras using Server Admin.

To control access to a workflow:

- 1 Open Server Admin.
- 2 Select Podcast Producer in the Computers & Services list.
- 3 Click Workflows.
- 4 Select a workflow in the Workflow list.
- 5 To restrict access to the workflow, click “Allow access to *workflow name* for the following users and groups.”
- 6 Click the (+) button to add users and groups to the list of users and groups that can access the selected workflow.

In the Users and Groups window, click Users and drag users to the list.

In the Users and Groups window, click Groups and drag groups to the list.

To delete users and groups from the list, select them and click (-).

- 7 Click Save.

To control access to a camera:

- 1 Open Server Admin.
- 2 In the Computers and Services list, select Podcast Producer.
- 3 Click Cameras.
- 4 Select a camera in the Cameras list.
- 5 To restrict access to the camera, click “Allow access to *camera name* for the following users and groups.”
- 6 Click the (+) button to add users and groups to the list of users and groups that can access the selected camera.
In the Users and Groups window, click Users and drag users to the list.
In the Users and Groups window, click Groups and drag groups to the list.
To delete users or groups from the list, select them and click (-).
- 7 Click Save.

Viewing Podcast Producer Service Logs

Podcast Producer service logging is important for security. With logs, you can monitor and track communication through the Podcast Producer service. Access the Podcast Producer service log, /Library/Logs/pcastserverd/application.log, using Server Admin.

To view the Podcast Producer service log:

- 1 Open Server Admin and connect to the server.
- 2 Click the triangle at the left of the server.
The list of services appears.
- 3 Click Podcast Producer.
- 4 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
#  
# View the Podcast Producer service log.  
# -----  
sudo tail /Library/Logs/pcastserverd/pcastserverd_out.log
```

Use this chapter to learn how to secure mail service.

Mail service is crucial in today's dispersed work environments. Protect your mail by using encryption, adaptive junk mail filtering, and virus detection.

Mail service in Snow Leopard Server allows network users to send and receive mail over your network or across the Internet.

Mail service sends and receives mail using the following standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP).

Mail service also uses a Domain Name System (DNS) service to determine the destination IP address of outgoing mail.

Snow Leopard Server uses Cyrus to provide POP and IMAP service. More information about Cyrus can be found at asg.web.cmu.edu/cyrus.

Snow Leopard Server uses Postfix as its mail transfer agent (MTA). Postfix fully supports SMTP. Your mail users will set their mail application's outgoing mail server to your Snow Leopard Server running Postfix, and access incoming mail from a Snow Leopard Server running incoming mail service. More information about Postfix can be found at www.postfix.org.

For more information about configuring mail service, see *Mail Service Administration*.

Disabling Mail Service

If your server is not to mail server, disable the mail service software. Disabling the service prevents potential vulnerabilities on your server. To disable mail service, turn off support for the IMAP, SMTP, and POP protocols that are not required. mail service is enabled by default (except in Advanced mode), so verification is recommended.

To disable mail service protocols:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the General tab.
- 4 Make sure at least one protocol (SMTP, POP, or IMAP) is enabled.
- 5 Click Stop Service in the menu bar.

When the service is turned on, the Stop Service button is available.

From the command line:

```
# -----
# Securing Mail Service
# -----  
  
# Disable mail service protocols
# -----
sudo serveradmin settings mail:imap:enable_pop = no
sudo serveradmin settings mail:imap:enable_imap = no
sudo serveradmin settings mail:postfix:enable_smtp = no
```

Configuring Mail Service for SSL

If mail service protocols are required, protect their communications using Secure Sockets Layer (SSL). SSL connections ensure that the data sent between your mail server and your users' mail clients is encrypted. This allows secure and confidential transport of mail messages across a local network.

SSL transport doesn't provide secure authentication. It provides secure transfer from your mail server to your clients. For secure authentication information, see *Open Directory Administration*.

For incoming mail, mail service supports secure mail connections with mail client software that requests them. If a mail client requests an SSL connection, mail service can comply if that option is enabled. mail service still provides non-SSL (unencrypted) connections to clients that don't request SSL. The configuration of each mail client determines whether it connects with SSL or not.

For outgoing mail, mail service supports secure mail connections between SMTP servers. If an SMTP server requests an SSL connection, mail service can comply if that option is enabled. mail service can still allow non-SSL (unencrypted) connections to mail servers that don't request SSL.

Enabling Secure Mail Transport with SSL

Mail service requires configuration to provide SSL connections automatically. The basic steps are as follows:

Step 1: Obtain a security certificate

This can be done in the following ways:

- Get a certificate from a Certificate Authority (CA).
- Generate a Certificate Signing Request (CSR) and create a keychain.
- Use the CSR to obtain a certificate from an issuing CA or create a self-signed certificate in Server Admin's Certificate Manager.
- Locate an existing certificate from a previous installation of Snow Leopard Server. If you have already generated a security certificate in a previous version of Leopard_Server, you can import it for use.

Step 2: Import the certificate into Server Admin's Certificate Manager

You can use Certificate Manager to drag and drop certificate information or you can provide Certificate Manager with the path to an existing installed certificate.

Step 3: Configure the service to use the certificate

For instructions for allowing or requiring SSL transport, see the following sections:

- "Configuring SSL Transport for POP Connections" on page 236
- "Configuring SSL Transport for IMAP Connections" on page 237
- "Configuring SSL Transport for SMTP Connections" on page 239

Enabling Secure POP Authentication

Your POP mail service can protect user passwords by allowing Authenticated POP (APOP) or Kerberos. When a user connects with APOP or Kerberos, the user's mail client software encrypts the user's password before sending it to your POP service.

Before configuring mail service to require secure authentication, make sure that users' mail applications and user accounts support the method of authentication you choose.

Before enabling Kerberos authentication for incoming mail service, you must integrate Snow Leopard with a Kerberos server. If you're using Snow Leopard Server for Kerberos authentication, this is already done for you. For more information, see *Open Directory Administration*.

If you want to *require* either of these authentication methods, enable only one method.

To set the POP authentication method:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 Click the APOP or Kerberos checkbox in the POP3 list.
- 6 Click Save.

From the command line:

```
# Set the POP authentication method:  
sudo serveradmin settings mail:imap:pop_auth_apop = no  
sudo serveradmin settings mail:imap:pop_auth_clear = no  
sudo serveradmin settings mail:imap:pop_auth_gssapi = no
```

Configuring SSL Transport for POP Connections

SSL transport enables mail transmitted over the network to be securely encrypted.

You can choose Require, Use, or Don't Use SSL for POP (and IMAP) connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for POP also sets it for IMAP.

To set SSL transport for POP connections:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 In the IMAP and POP SSL pop-up menus, select Require or Use to enable (or Don't Use to disable).
- 6 Select the certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
- 7 Click Save.

From the command line:

```
# Set SSL transport for POP connections:  
sudo serveradmin settings mail:imap:tls_server_options = "use"
```

Enabling Secure IMAP Authentication

Your IMAP mail service can protect user passwords by requiring that connections use a secure method of authentication. You can choose CRAM-MD5 or Kerberos v5 authentication.

When a user connects with secure authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Make sure that your users' mail applications and user accounts support the method of authentication you choose.

If you configure mail service to require CRAM-MD5, you must set mail accounts to use a Snow Leopard Server Password Server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Snow Leopard Server with a Kerberos server. If you're using Snow Leopard Server for Kerberos authentication, this is done for you. For instructions, see *Open Directory Administration*.

If you want to *require* any of these authentication methods, enable only one method.

To set secure IMAP authentication:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 Select CRAM MD-5 or Kerberos (as needed) in the IMAP section.
- 6 Click Save.

From the command line:

```
# Set secure IMAP authentication:  
sudo serveradmin settings mail:imap:imap_auth_login = no  
sudo serveradmin settings mail:imap:imap_auth_plain = no  
sudo serveradmin settings mail:imap:imap_auth_gssapi = no  
sudo serveradmin settings mail:imap:imap_auth_clear = no  
sudo serveradmin settings mail:imap:imap_auth_cram_md5 = no
```

Configuring SSL Transport for IMAP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

Setting SSL transport for IMAP also sets it for POP.

To configure SSL transport for IMAP connections:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 From the pop-up menus in the IMAP and POP SSL section click Require or Use to enable (Don't Use to disable).
- 6 Select the Certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
- 7 Click Save.

From the command line:

```
# Configure SSL transport for IMAP connections (same as POP)
sudo serveradmin settings mail:imap:tls_server_options = "use"
```

Enabling Secure SMTP Authentication

Your server can guard against being an open relay by allowing SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) You can configure mail service to require secure authentication using CRAM-MD5 or Kerberos.

You can also allow the less secure plain and login authentication methods, which don't encrypt passwords, if some users have mail client software that doesn't support secure methods.

If you configure mail service to require CRAM-MD5, mail users' accounts must be set to use a password server that has CRAM-MD5 enabled. For information, see *Open Directory Administration*.

Before enabling Kerberos authentication for incoming mail service, you must integrate Snow Leopard Server with a Kerberos server. If you're using Snow Leopard Server for Kerberos authentication, this is done for you. For instructions, see *Open Directory Administration*.

Enabling SMTP authentication will:

- Make your users authenticate with their mail client before accepting mail to send.
- Frustrate mail server abusers trying to send mail without your consent through your system.

If you want to *require* any of these authentication methods, enable only one method.

To allow secure SMTP authentication:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 In the SMTP section, click the CRAM MD-5 or Kerberos checkbox.
- 6 Click Save.

From the command line:

```
# Allow secure SMTP authentication:  
sudo serveradmin settings mail:postfix:smtpd_sasl_auth_enable = yes  
sudo serveradmin settings mail:postfix:smtpd_use_pw_server = "yes"  
sudo serveradmin settings  
    mail:postfix:smtpd_pw_server_security_options:_array_index:0 =  
        "gssapi"  
sudo serveradmin settings  
    mail:postfix:smtpd_pw_server_security_options:_array_index:1 = "cram-  
        md5"  
sudo serveradmin settings  
    mail:postfix:smtpd_pw_server_security_options:_array_index:2 = "login"  
sudo serveradmin settings  
    mail:postfix:smtpd_pw_server_security_options:_array_index:3 = "plain"
```

Configuring SSL Transport for SMTP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use.

To configure SSL transport for SMTP connections:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Advanced tab.
- 4 Select Security.
- 5 In the SMTP SSL section, click Require or Use to enable (or Don't Use to disable).
- 6 Select the certificate you want to use from the corresponding pop-up menu, if you are using or requiring SSL.
- 7 Click Save.

From the command line:

```
# Configure SSL transport for SMTP connections:  
sudo serveradmin settings mail:postfix:smtpd_use_tls = "yes"
```

Using ACLs for Mail Service Access

Access Control Lists (ACLs) are a method of designating service access to specific users or groups on an individual basis. For example, you can use an ACL to allow only one user to access a file server or shell login, without allowing other users on the server to access it.

Mail services are different from services that traditionally use ACLs for determining service access. mail service is already specified on a per-user basis. Either you have a mail account on a server or you don't. Being a user on a server doesn't automatically confer access to mail storage and retrieval.

Some administrators find it easier to designate mail access using ACLs if they are doing all their other configuration using ACLs. They also might have mixed network environments that necessitate using ACLs to assign mail access.

Snow Leopard Server allows you to enable mail access for users using the Access tab in a server's Server Admin listing. If you enabled user access via Server Admin and traditional mail access using Workgroup Manager, the settings interact in the following manner:

Access via ACL	Access via Workgroup Manager	Result
On	On	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
On	Off	User has mail access granted according to the IMAP or POP settings in the General Settings Mail panel in Server Admin.
Off	On	User has mail access granted according to his or her user record settings in Workgroup Manager. This is the default.
Off	Off	User has no mail access.

To enable a user's mail access using ACLs:

- 1 In Server Admin, select the server that has mail service running and then click Settings.
- 2 Select Access, then click Services.
- 3 Select Mail from the Services list.
- 4 Deselect “Use same access for all services.”
- 5 Select “Allow only users and group below.”

- 6 Click the Add (+) button to reveal a Users and Groups list.
- 7 Drag the user or group to the access list.
- 8 Click Save.

From the command line:

```
# Enable a user's mail access using ACLs
sudo dseditgroup -o edit -a $USER -t user com.apple.access_mail
```

Limiting Junk Mail and Viruses

You can configure mail service to decrease the volume of unsolicited commercial mail, also known as junk mail (or spam), and mail containing viruses. You can take steps to block junk mail or viruses that are sent to mail users. Additionally, you can secure your server against use by mail service abusers, who try to use your resources to send junk mail to others.

You can also prevent senders of junk mail from using your server as a relay point. A relay point or open relay is a server that unselectively receives and forwards mail addressed to other servers. An open relay sends mail from any domain to any domain.

Junk mail senders exploit open relay servers to avoid having their SMTP servers blacklisted as sources of junk mail. You don't want your server blacklisted as an open relay because other servers may reject mail from your users.

There are two main methods of preventing viruses and junk mail passing through or into your mail system. Using both methods will help ensure your mail system integrity.

The two methods are:

- “Connection Control” on page 241
- “Mail Screening” on page 245

Connection Control

This method of prevention controls which servers can connect to your mail system and what those servers must do to send mail through your mail system. Your mail service can do any of the following to exercise connection control:

- Require SMTP authentication
- Restrict SMTP relay, allowing relay only by approved servers
- Reject SMTP connections from disapproved servers
- Reject mail from blacklisted servers
- Filter SMTP connections

These methods are explained on the following pages.

Requiring SMTP Authentication

If your mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server.

Although SMTP authentication applies primarily to mail relay, your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they can't send mail to remote servers. Mail sent from external mail servers and addressed to local recipients is still accepted and delivered.

To require SMTP authentication, see "Enabling Secure SMTP Authentication" on page 238.

Restricting SMTP Relay

Your mail service can restrict SMTP relay by allowing only approved hosts to relay mail. You create the list of approved servers.

Approved hosts can relay through your mail service without authenticating. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All hosts, approved or not, can deliver mail to your local mail users without authenticating.

Your mail service can log connection attempts made by hosts not on your approved list.

To restrict SMTP relay:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Relay tab.
- 4 Click the "Accept SMTP relays only from these" checkbox.
- 5 Edit the list of hosts:
 - Click the Add (+) button to add a host to the list.
 - Click the Remove (-) button to delete a selected host from the list.
 - Click the Edit (/) button to change a selected host from the list.

When adding to the list, you can use a variety of notations.

- Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21.
- Enter a host name, such as mail.example.com.
- Enter an Internet domain name, such as example.com.

From the command line:

```
# Restrict SMTP relay:  
sudo serveradmin settings mail:postfix:mynetworks_enabled = yes
```

SMTP Authentication and Restricted SMTP Relay Combinations

The following table describes the results of using SMTP authentication and restricted SMTP relay in various combinations.

SMTP requires authentication	Restricted SMTP relay	Result
On	Off	All mail servers must authenticate before your mail service accepts mail for relay. Your local mail users must also authenticate to send mail out.
On	On	Approved mail servers can relay without authentication. Servers you haven't approved can relay after authenticating with your mail service.
Off	On	Your mail service can't be used for open relay. Approved mail servers can relay (without authenticating). Servers that you haven't approved can't relay unless they authenticate, but they can deliver to your local mail users. Your local mail users don't need to authenticate to send mail. This is the most common configuration.

Rejecting SMTP Connections from Specific Servers

Your mail service can reject unauthorized SMTP connections from hosts on a disapproved-hosts list that you create. Mail traffic from hosts on this list is denied and SMTP connections are closed after posting a 554 SMTP connection refused error.

To reject unauthorized SMTP connections from specific servers:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Relay tab.
- 4 Click the “Refuse all messages from these” checkbox.
- 5 Edit the list of servers:
 - Click the Add (+) button to add a host to the list.
 - Click the Remove (-) button to delete the selected host from the list.
 - Click the Edit (/) button to change the selected host from the list.

When adding to the list, you can use the following notations:

- Enter a single IP address or the network/netmask pattern, such as 192.168.40.0/21.
- Enter a host name, such as mail.example.com.
- Enter an Internet domain name, such as example.com.

From the command line:

```
# Reject unauthorized SMTP connections:  
sudo serveradmin settings mail:postfix:smtp_reject_list_enabled = yes  
sudo serveradmin settings mail:postfix:smtp_reject_list:_array_index:0 =  
    "$NETWORK"
```

Rejecting Mail from Blacklisted Senders

Your mail service can reject mail from SMTP servers that are blacklisted as open relays by a Real-time Blacklist (RBL) server. Your mail service uses an RBL server that you specify. RBLs are also called *black-hole servers*.

Blocking unsolicited mail from blacklisted senders might not be completely accurate. Sometimes it prevents valid mail from being received.

To reject mail from blacklisted senders:

- 1 In Server Admin, select Mail in the Computers & Services pane.
- 2 Click Settings.
- 3 Select the Relay tab.
- 4 Click the “Use these junk mail rejection servers” checkbox.
- 5 Edit the list of servers by adding the DNS name of an RBL server:
 - Click the Add (+) button to add a server to the list, then enter the domain name of a RBL server, such as rbl.example.com.
 - Click the Remove (-) button to delete a server from the list.
 - Click the Edit (/) button to change a server.

From the command line:

```
# Reject mail from blacklisted senders:  
sudo serveradmin settings mail:postfix:black_hole_domains:_array_index:0 =  
    "$BLACKLIST_SERVER"  
sudo serveradmin settings mail:postfix:maps_rbl_domains_enabled = yes
```

Filtering SMTP Connections

You can use firewall service of Snow Leopard Server to allow or deny access to your SMTP mail service from specific IP addresses. Filtering disallows communication between an originating host and your mail server. mail service doesn't receive the incoming connection and no SMTP error is generated or sent back to the client.

To filter SMTP connections:

- 1 In Server Admin, select Firewall in the Computers & Services pane.
- 2 Create a firewall IP filter using the instructions in *Network Services Administration*, using the following settings:
 - Access: denied
 - Port number: 25 (or your incoming SMTP port, if you use a nonstandard port)
 - Protocol: TCP
 - Source: the IP address or address range you want to block
 - Destination: your mail server's IP address
- 3 If needed, log the packets to monitor the SMTP abuse.
- 4 Add more filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information about firewall service, see *Network Services Administration*.

Mail Screening

After a mail delivery connection is made and the message is accepted for local delivery (relayed mail is not screened), the mail server can screen it before delivery.

Snow Leopard Server uses SpamAssassin (from spamassassin.apache.org) to analyze the text of a message, and gives it a probability rating for being junk mail.

No junk mail filter is 100% accurate in identifying unwanted mail. For this reason the junk mail filter in Snow Leopard Server doesn't delete or remove junk mail from being delivered. Instead, it marks the mail as potential junk mail.

The user can then decide if it's really unsolicited commercial mail and deal with it accordingly. Many mail clients use the ratings that SpamAssassin adds as a guide in classifying mail for the user.

Snow Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can deal with it in several ways, as described in "Enabling Junk Mail Screening (Bayesian Filters)" on page 245. Virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

Enabling Junk Mail Screening (Bayesian Filters)

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

Bayesian mail filtering is the classification of mail messages based on statistics. Each message is analyzed and word frequency statistics are saved. Mail messages that have more of the same words as those in junk mail receive a higher marking of probability that they are also junk mail. When the message is screened, the server adds a header ("X-Spam-Level") with the junk mail probability score.

For example, let's say you have 400 mail messages where 200 of them are junk mail and 200 are good mail. When a message arrives, its text is compared to the 200 junk mail and the 200 good messages. The filter assigns the incoming message a probability of being junk or good, depending on what group it most resembles.

Bayesian filtering has shown itself to be a very effective method of finding junk mail, if the filter has enough data to compare. One of the strengths of this method is the more mail you get and classify (a process called training), the more accurate the next round of classification is. Even if junk mail senders alter their mailings, the filter takes that into account the next time around.

To enable junk mail screening:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Filters tab.
- 4 Select Scan Mail for Junk Mail.
- 5 Set the level of permissiveness (Cautious, Moderate, Aggressive).

The permissiveness meter sets how many junk mail flags can be applied to a message before it is processed as junk mail. If you set it to "Least permissive," mildly suspicious mail is tagged and processed as junk mail. If you set it to "Most permissive" it takes a high score (in other words, many junk mail characteristics) to mark it as junk.

- 6 Decide how to deal with junk mail messages.
 - *Bounced*: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
 - *Deleted*: Deletes the message without delivery. You can optionally send a mail notification of the bounce to a mail account, probably the postmaster.
 - *Delivered*: Delivers the message even though it's probably junk mail. You can optionally add text to the subject line, indicating that the message is probably junk mail, or encapsulate the junk mail as a MIME attachment.
 - *Redirected*: Delivers the message to someone other than the intended recipient.
- 7 Choose how often to update the junk mail database updated, if desired.
- 8 Click Save.

For an explanation of other options, see "Filtering Mail by Language and Locale" on page 248.

From the command line:

```
# Enable junk mail screening:  
sudo serveradmin settings mail:postfix:spam_scan_enabled = yes
```

Manually Training the Junk Mail Filter

It's important to teach the filter what is and isn't junk mail. Initially, the filter won't be very accurate at marking junk mail, but you can train it to do better. Accurate training requires a large sample, so a minimum of 200 messages of each type is advised.

To train the filter:

- 1 Choose a mailbox of 200 messages made of only junk mail.
- 2 Use Terminal and the filter's command-line training tool to analyze it and remember it as junk mail using the following command:
`sudo sa-learn --showdots --spam <junk mail directory>/*`
- 3 Choose a mailbox of 200 messages made of only good mail.
- 4 Use Terminal and the filter's command-line training tool to analyze it and remember it as good mail using the following command:
`sudo sa-learn --showdots --ham <junk mail directory>/*`

If the junk mail filter fails to identify a junk mail message, train it again so it can do better next time. Use `sa-learn` again with the `--spam` argument on the mislabeled message. Likewise, if you get a false positive (a good message marked as junk mail), use `sa-learn` again with the `--ham` argument to further train the filter.

From the command line:

```
# Train the filter:  
sudo sa-learn --showdots --spam $JUNK_DIRECTORY/*  
sudo sa-learn --showdots --ham $NON_JUNK_DIRECTORY/*
```

Automatically Training the Junk Mail Filter

The junk mail filter must be told what is and isn't junk mail. Snow Leopard Server provides a method of automatically training the filter with the help of mail users.

The server runs an automated command at 1 am (a launchd recurring event) that scans two specially named mail users' in boxes. It runs SpamAssassin's sa-learn tool on the contents of the in boxes and uses the results for its adaptive junk mail filter.

To automatically train the junk mail filter:

- 1** Enable junk mail filtering.
See "Enabling Junk Mail Screening (Bayesian Filters)" on page 245.
- 2** Create two local accounts: junkmail and notjunkmail.
- 3** Use Workgroup Manager to enable them to receive mail.
- 4** Instruct your mail users to redirect junk mail messages that have not been tagged as junk mail to junkmail@<yourdomain>.
- 5** Instruct your mail users to redirect real mail messages that were wrongly tagged as junk mail to notjunkmail@<yourdomain>.

Each day at 1 am, the junk mail filter will learn what is junk and what was mistaken for junk, but is not.

- 6** Delete the messages in the junkmail and notjunkmail accounts daily.

From the command line:

```
# Automatically train the junk mail filter:  
sudo /etc/mail/spamassassin/learn_junk_mail
```

Filtering Mail by Language and Locale

You can filter incoming mail based on locales or languages. Mail messages composed in foreign text encodings are often erroneously marked as junk mail. You can configure your mail server to not mark messages from designated originating countries or languages as junk mail.

To allow mail by language and locale:

- 1** In Server Admin, select a computer in the Servers list, then select Mail.
- 2** Click Settings.
- 3** Select the Filters tab.
- 4** Select Scan Email for Junk Mail.
- 5** Click the Edit (/) button next to Accepted Languages to change the list, select the language encodings to allow as non-junk mail, and click OK.

- 6 Click the Edit (/) button next to Accepted Locales to change the list, select the country codes to allow as non-junk mail, and click OK.
- 7 Click Save.

From the command line:

```
# Allow mail by language and locale:  
sudo serveradmin settings mail:postfix:spam_ok_languages = "en fr de"  
sudo serveradmin settings mail:postfix:spam_ok_locales = "en"
```

Enabling Virus Screening

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

Snow Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages for viruses. If a suspected virus is found, you can choose to deal with it several ways, as described below. The virus definitions are kept up to date (if enabled) via the Internet using a process called freshclam.

To enable virus screening:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Filters tab.
- 4 Select Scan Email for Viruses.
- 5 Decide how to deal with messages containing viruses.

Bounced: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account (probably the domain's postmaster) and notify the intended recipient.

Deleted: Deletes the message without delivery. You can optionally send a mail notification to some mail account, probably the postmaster, as well as the intended recipient.

Quarantined: Delivers the message to a directory for further analysis. You can optionally send a mail notification of the quarantine to some mail account, probably the postmaster.

- 6 Choose if you want to notify the intended recipient if the message was filtered.
- 7 Choose how often to update the virus database.
A minimum of twice a day is suggested. Some administrators choose eight times a day.
- 8 Click Save.

From the command line:

```
# Enable virus screening:  
sudo serveradmin settings mail:postfix:virus_scan_enabled = yes
```

Viewing Mail Service Logs

Mail service maintains the following logs that you can view in Server Admin. The file location for each log is shown beneath the Show pop-up menu.

- *Mail Access*: General mail service information goes into this log.
- *IMAP log*: IMAP-specific activity goes into this log.
- *POP log*: POP specific activity goes into this log.
- *SMTP log*: SMTP specific activity goes into this log.
- *Mailing List logs*: The logs record Mailmain's activity, including service, error, delivery failures, postings, and subscriptions.
- *Junk Mail and Virus logs*: These show activity for mail filtering, including logs for virus definition updates (freshclam log), virus scanning (clamav log), and mail filtering (amavis log).

Logs can be refined by using the text filter box in the window.

To view a mail service log:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click the Logs button.
- 3 From the View pop-up menu choose a log type.
- 4 Click Save.

From the command line:

```
# View a mail service log:  
sudo tail /var/log/mail.log
```

Use this chapter to learn how to use the antivirus services built into your system to detect and remove viruses.

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

Snow Leopard Server uses ClamAV (from www.clamav.net) to scan mail messages and attachments for viruses. If a suspected virus is found, ClamAV deletes the message or quarantines it to a specified directory on the server for further analysis.

The virus definitions are kept up to date (if enabled) via the Internet using a process called `freshclam`.

In addition to using antivirus tools, you should develop computer usage habits that prevent 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.

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 tool supports it, enable automatic downloading of virus definitions.

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

Securely Configuring and Managing Antivirus Services

This section describes how to securely configure and manage antivirus services.

Enabling Virus Scanning

Before you can benefit from mail screening, it must be enabled. While enabling screening, you configure screening parameters.

To enable virus screening:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click Settings.
- 3 Select the Filters tab.
- 4 Select Scan Email for Viruses.
- 5 Decide how to deal with junk mail messages.

Bounced: Sends the message back to the sender. You can optionally send a mail notification of the bounce to a mail account (probably the domain's postmaster) and notify the intended recipient.

Deleted: Deletes the message without delivery. You can optionally send a mail notification to some mail account, probably the postmaster, as well as the intended recipient.

Quarantined: Delivers the message to a directory for further analysis. You can optionally send a mail notification of the quarantine to some mail account, probably the postmaster.

- 6 Choose if you want to notify the intended recipient if the message was filtered.
- 7 Choose how often to update the virus database.

A minimum of twice a day is suggested. Some administrators choose eight times a day.

- 8 Click Save.

From the command line:

```
# -----
# Securing Antivirus Services
# -----  
  
# Enable virus screening
sudo serveradmin settings mail:postfix:virus_scan_enabled = yes
```

Managing ClamAV with ClamXav

You can use ClamXav, a free GUI front-end to the ClamAV open source virus checker.

This tool allows you to:

- Update virus definitions
- Scan files and folders for viruses

ClamXav performs the following tasks:

- Logs results to a log file
- Places infected files into quarantine
- Monitors folders for changes to their contents

You can access ClamXav services through contextual pop-up menus in the Finder.

Viewing Antivirus Services Logs

Mail service maintains the following junk mail and virus logs that you can view in Server Admin. The file location for each log is shown beneath the Show pop-up menu.

- Junk Mail/Virus Scanning (/var/log/amavis.log)
- Virus (/var/log/clamav.log)
- Virus Database Updates (/var/log/freshclam log)

To view a virus service log:

- 1 In Server Admin, select a computer in the Servers list, then select Mail.
- 2 Click the Logs button.
- 3 From the View pop-up menu choose a log type.
- 4 Click Save.

From the command line:

```
# View a virus log:  
sudo tail /var/log/amavisd.log
```

Use this chapter to learn how to secure file services.

Securely configuring file services is an important step in the process of protecting your private data from network attacks.

Snow Leopard Server's cross-platform file sharing services help groups work more efficiently

by letting them share resources, archive projects, exchange and back up important documents, and conduct other file-related activities.

Sharing files over a network opens your computers up to a host of vulnerabilities. With file services enabled, you are allowing access to files and folders on your server (also called share points).

For more information about configuring file services, see *File Services Administration*.

Security Considerations

The most effective method of securing your network is to assign correct privileges for each file, folder, and share point you create.

Restricting Access to File Services

Use Service Access Control Lists (SACLs) to restrict access to AFP, FTP, and SMB services.

Restricting Access to Everyone

Be careful when creating and granting access to share points, especially if you're connected to the Internet. Granting access to Everyone or to World (in NFS service) can expose your data to anyone on the Internet. For NFS, it is recommended that you do not export volumes to World and that you use Kerberos to provide security for NFS volumes.

Restricting Access to NFS Share Points

NFS share points without the use of Kerberos don't have the same level of security as AFP and SMB, which require user authentication (entering a user name and password) to gain access to a share point's contents.

If you have NFS clients, consider setting up a share point to be used only by NFS users, or configure NFS with Kerberos. NFS doesn't support SACLs. For more information, see "Protocol Security Comparison" on page 256.

Restricting Guest Access

When you configure file service, you can turn on guest access. Guests are users who connect to the server anonymously without entering a user name or password. Users who connect anonymously are restricted to files and folders that have privileges set to Everyone.

To protect your information from unauthorized access, and to prevent people from introducing software that might damage your information or equipment, take the following precautions by using File Sharing in Server Admin:

- Depending on the controls you want to place on guest access to a share point, consider the following options:
 - Set privileges for Everyone to None for files and folders that guest users shouldn't access. Items with this setting can be accessed only by the item's owner or group.
 - Put files available to guests in one folder or set of folders and then assign the Read Only privilege to the Everyone category for that folder and each file in it.
 - Assign Read & Write privileges to the Everyone category for a folder only if guests must be able to change or add items in the folder. Make sure you keep a backup copy of information in this folder.
- Don't export NFS volumes to World. Restrict NFS exports to a subnet or a specific list of computers.
- Disable access to guests or anonymous users over AFP, FTP, and SMB using Server Admin.
- Share individual folders instead of entire volumes. The folders should contain only those items you want to share.

Restricting File Permissions

Before a folder is shared, its permissions should be restricted as much as possible. Permissions on share points set as user home folders are particularly important. By default, users' home folders are set to allow any other user to read their contents.

For more information about setting file permissions, see Chapter 6, "Securing System Preferences."

Protocol Security Comparison

When sharing network resources, configure your server to provide the necessary security.

AFP and SMB provide some level of encryption to secure password authentication. AFP and SMB do not encrypt data transmissions over the network so you should only use them on a securely configured network.

FTP does not provide password or data encryption. When using FTP, make sure your network is securely configured. Instead of using FTP, consider using the `scp` or `sftp` command-line tools. These tools securely authenticate and securely transfer files.

The following table provides a comparison of the protocols and their authentication and encryption capabilities.

Protocol	Authentication	Data Encryption
AFP	Cleartext and encrypted (Kerberos) passwords.	Not encrypted and data is visible during transmission.
NFS	Encrypted (Kerberos) password and system authentication.	Can be configured to encrypt data transmission.
SMB	Cleartext and encrypted (NTLM v1, NTLM v2, LAN Manager, and Kerberos) passwords.	Not encrypted and data is visible during transmission.
FTP	Cleartext passwords.	Not encrypted. Data is sent as cleartext.

Disabling File Sharing Services

Unless you use the server as a file server, disable file sharing services. Disabling these services prevents your computer from being used by an attacker to access other computers on your network.

To disable file sharing services:

- 1 Open Server Admin and connect to the server.
- 2 Select the file sharing protocol in the Computers & Services list.
You can choose AFP, FTP, NFS, or SMB.
- 3 Click “Stop (protocol name)” below the Computers & Services list.
- 4 Repeat for each protocol.

From the command line:

```
# -----
# Securing File Services
# -----  
  
# Disable file sharing services.  
sudo serveradmin stop afp  
sudo serveradmin stop smb  
sudo serveradmin stop ftp  
sudo serveradmin stop nfs
```

Choosing a File Sharing Protocol

If you require file sharing services, you must choose which file sharing protocols are needed before configuring the services. The protocol is configured for the folders you are sharing, called share points. The share points are created and configured using Workgroup Manager.

Most installations only need one file sharing protocol, and you should use as few protocols as possible. Limiting the number of protocols used by a server limits its exposure to vulnerabilities discovered in those protocols. The protocol choices are:

- **Apple Filing Protocol (AFP):** AFP is the preferred method of file sharing for Macintosh or compatible client systems. AFP supports authentication of clients, and also supports encrypted network transport using SSH.
- **File Transfer Protocol (FTP):** FTP should generally not be used for file sharing. Use the SFTP feature of SSH instead. SFTP provides a secure means of authentication and data transfer, while FTP does not.
The only situation where FTP is acceptable is when the server must act as a file server for anonymous users. This might be necessary over WANs, where there is no concern for the confidentiality of data and responsibility for the integrity of the data rests with its recipient.
- **Network File System (NFS):** NFS is a common file sharing protocol for UNIX computers. Avoid using NFS, because it does not perform authentication of its clients—it grants access based on client IP addresses and file permissions. Using NFS may be appropriate if the client computer administration and the network are trusted.

- **Microsoft Windows Server Message Block (SMB):** SMB is the native file sharing protocol for Microsoft Windows. Avoid using SMB—it supports authentication but does not support encrypted network transport, and it uses NTLMv1 and NTLMv2 encryption, both of which are weak password hashing schemes. SMB may be an appropriate protocol for Windows clients when the network between the server and client is not at risk for eavesdropping.

Each protocol is appropriate for specific situations. Deciding which protocol to use depends on the clients and networking needs. After you choose a protocol for file sharing, you must configure the file sharing protocol.

If no share points are shared with a protocol, disable the service that runs that protocol using Server Admin. The NFS service stops when no share points specify its use.

Configuring AFP File Sharing Service

Apple File Service, which uses AFP, lets you share files among Macintosh clients. Because it provides authentication and encryption, AFP service is the preferred file sharing method for Macintosh or compatible clients.

Note: Encryption does not apply to automatically mounted home folders, where only authentication is provided.

To securely configure AFP Service:

- 1 Open Server Admin and connect to the server.
- 2 Select AFP in the Computers & Services list.
- 3 Click Settings.
- 4 Click General.
- 5 Enter the login greeting according to site policy.
- 6 Click Access.
- 7 For Authentication, choose “Kerberos” if your system is integrated into a Kerberos system; otherwise, choose “Standard.”
- 8 Deselect “Enable administrator to masquerade as any registered user.”
- 9 Under Maximum Connections, enter the largest expected number for Client Connections.
- 10 Click Logging.
- 11 Select “Enable access Log” to enable logging.
- 12 Select “Archive every __ day(s)” and set the frequency to three days or according to your organization’s requirements.

- 13** Select “Login” and “Logout” to include events in the access log.
If you need stronger accounting, select the other events.
- 14** Under Error Log, select “Archive every __ day(s)” and set the frequency according to your organization’s requirements.
- 15** Click Idle Users and configure Idle Users settings:
 - Deselect “Allow clients to sleep __ hour(s) - will not show as idle.”
 - Select “Disconnect idle users after __ minute(s)” and enter a value in the text field to mitigate risk from a computer accidentally being left unattended.
 - Deselect Guests, Administrators, Registered Users, and Idle Users who have open files.
 - Enter a “Disconnect Message” notice according to site policy.
- 16** Click Save.
- 17** Click Start AFP.
- 18** For additional security enhancements, further restrict AFP by using SACLs and firewall rules.

These are configured based on your organization’s network environment:

- You can configure SACLs to restrict AFP access to specific users or groups. For more information, see “Setting Service Access Control Lists (SACLs)” on page 183.
- You can configure firewall rules that prevent AFP connections from unintended sources. For more information, see “Creating Firewall Service Rules” on page 216.

From the command line:

```
# Securely configure AFP service:  
sudo serveradmin settings afp:registerNSL = no  
sudo serveradmin settings afp:attemptAdminAuth = no  
sudo serveradmin settings afp:clientSleepOnOff = no  
sudo serveradmin settings afp:idleDisconnectOnOff = yes  
sudo serveradmin settings afp:authenticationMode = "kerberos"  
sudo serveradmin settings afp:activityLog = yes  
sudo serveradmin settings afp:guestAccess = no
```

Configuring FTP File Sharing Service

If authentication of users is possible, use the SFTP portion of SSH instead of FTP to securely transmit files to and from the server. For more information, see “Transferring Files Using SFTP” on page 191.

FTP is acceptable only if its anonymous access feature is required, which allows unauthenticated clients to download files. The files are transferred unencrypted over the network and no authentication is performed.

Although the transfer does not guarantee confidentiality or integrity to the recipient, it is appropriate in some cases. If this capability is not specifically required, disable it.

To configure FTP to provide anonymous FTP downloads:

- 1 Open Server Admin and connect to the server.
- 2 Select FTP in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 In "Disconnect client after __ login failures," enter 1.

Even though authenticated connections are not accepted, logins should fail quickly if accidentally activated.

- 5 Enter a mail address specially set up to handle FTP administration—for example, `ftpadmin@hostname.com`.
- 6 Under Access, select "Kerberos" for Authentication.
If a Kerberos server is not set up, the authentication process is blocked.
- 7 In "Allow a maximum of __ authenticated users," enter 1.

The GUI does not allow setting this to 0, but authenticated users are disabled in later steps.

- 8 Select "Enable anonymous access."

Anonymous access prevents user credentials from being sent openly over the network.

Important: Before selecting this option, review the privileges assigned to your share points under File Privileges in the Sharing pane to make sure there are no security holes.

Anonymous users can log in using the name "ftp" or "anonymous." They do not need a password to log in, but they are prompted to enter their email address.

- 9 Determine a maximum number of anonymous users and enter the number in "Allow a maximum of __ anonymous users."
- 10 Under File conversion, deselect "Enable MacBinary and disk image auto-conversion."
- 11 Click Messages.
- 12 Select "Show Welcome Message" and enter a welcome message according to site policy.
- 13 Select "Show Banner Message" and enter a banner message according to site policy.
Do not reveal software information, such as operating system type or version, in the banner.

- 14** Click Logging.
- 15** Select all options under “Log Authenticated Users” and “Log Anonymous Users.”

Even though authenticated users are not allowed to log in, their attempts should be logged so corrective action can be taken.
- 16** Click Advanced.
- 17** Set “Authenticated users see” to FTP Root and Share Points.

Authenticated users and anonymous users see the same FTP root.
- 18** Verify that “FTP root” is set to the /Library/FTPServer/FTPRoot/ folder.
- 19** Click Save.
- 20** Click Start FTP.
- 21** Open the /Library/FTPServer/FTPRoot/ folder and drag the contents (Users, Groups, Public) to the trash.
- 22** Drag the files to share with anonymous users to the /Library/FTPServer/FTPRoot/ folder.
- 23** Verify that the file permissions for the /Library/FTPServer/FTPRoot/ folder do not allow public write access.
- 24** Open the file /Library/FTPServer/Configuration/ftpaccess for editing.
- 25** Delete lines that begin with “upload.”

The following two line are present by default:

```
upload /Library/FTPServer/FTPRoot /uploads yes ftp daemon 0666 nodirs  
upload /Library/FTPServer/FTPRoot /uploads/mkdirs yes ftp daemon 0666 dirs  
0777
```

- 26** Insert the following line to prevent advertisement of operating system and version information:

```
greeting terse
```
- 27** Insert the following lines to prevent users from authenticating.

```
deny-gid %--99 %65535  
deny-uid %--99 %65535  
allow-gid ftp  
allow-uid ftp
```

This forces users to access FTP anonymously, protecting their login credentials.
- 28** For additional security enhancements, you can further restrict the FTP service by using SACLs and firewall rules.

These are configured based on your organization’s network environment.

 - You can configure SACLs to restrict FTP access to specific users or groups. For more information about configuring SACLs, see “Setting Service Access Control Lists (SACLs)” on page 183.

- You can configure firewall rules that prevent FTP connections from unintended sources. For more information, see “Creating Firewall Service Rules” on page 216.

From the command line:

```
# Configure FTP to provide anonymous FTP downloads:  
sudo serveradmin settings ftp:logSecurity:anonymous = yes  
sudo serveradmin settings ftp:logSecurity:guest = yes  
sudo serveradmin settings ftp:logSecurity:real = yes  
sudo serveradmin settings ftp:maxRealUsers = 1  
sudo serveradmin settings ftp:enableMacBinAndDmgAutoConversion = no  
sudo serveradmin settings ftp:authLevel = "KERBEROS"  
sudo serveradmin settings ftp:anonymousAccessPermitted = yes  
sudo serveradmin settings ftp:bannerMessage = "$BANNER"  
sudo serveradmin settings ftp:maxAnonymousUsers = 500  
sudo serveradmin settings ftp:administratorEmailAddress = "user@domain.com"  
sudo serveradmin settings ftp:logCommands:anonymous = yes  
sudo serveradmin settings ftp:logCommands:guest = yes  
sudo serveradmin settings ftp:logCommands:real = yes  
sudo serveradmin settings ftp:loginFailuresPermitted = 1  
sudo serveradmin settings ftp:welcomeMessage = "$WELCOME"
```

Configuring NFS File Sharing Service

NFS does not support user name and password authentication. It relies on client IP addresses to authenticate users, and on client enforcement of permissions. This is not a secure approach in most networks. Therefore, use NFS only if you are on a LAN with trusted client computers, or if you are in an environment that can't use Apple file sharing or Windows file sharing.

The NFS server included with Snow Leopard Server lets you limit access to a share point based on a client’s IP address. Restrict access to a share point exported using NFS to those clients that require it. You can reshare NFS mounts using AFP, Windows, and FTP so that users can access NFS volumes in a more restricted fashion.

To configure and start NFS service, use Server Admin. For information about how to setup and restrict NFS service, see “NFS Share Points” on page 268.

For additional security enhancements, you can further restrict NFS service by using firewall rules. You can configure firewall rules that prevent AFP connections from unintended sources.

For more information, see “Creating Firewall Service Rules” on page 216. Rules are configured based on your organization’s network environment.

Configuring SMB File Sharing Service

If share points need to use SMB, activate Windows file service and configure it. Support for SMB is provided by the open source Samba project, which is included with Snow Leopard Server.

SMB uses NTLMv1 and NTLMv2 encryption, which are very weak password hashing schemes. For more information about configuring the Samba software, go to www.samba.org.

To securely configure Windows file sharing service:

- 1 Open Server Admin and connect to the server.
- 2 Select SMB in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 Choose the Role according to operational needs.

If the server shares files but does not provide authentication services, "Standalone Server" is the relevant choice.

- 5 Fill in the text fields appropriately, leaving the Description field blank.

It is helpful for the computer name to match the host name (without the domain name). The Workgroup name depends on the configuration of Windows domains on your subnet.

- 6 Click Access.
- 7 Deselect "Allow Guest access."
- 8 For "Client connections," select "__ maximum" and enter the maximum number of client connections expected.

The Graphs pane shows current usage, which can help you adjust the number of connections for your network.

- 9 Click Logging.
- 10 Change "Log Detail" to at least "medium" to capture authentication failures.
- 11 Click Advanced.
- 12 Under Services, deselect "Workgroup Master Browser" and "Domain Master Browser" unless these services are required.
- 13 Select Off for WINS registration.
- 14 Click Save.
- 15 Click Start SMB.
- 16 For additional security enhancements, further restrict the Windows service by using SACLs and firewall rules.

These are configured based on your organization's network environment:

- You can configure SACLs to restrict Windows access to specific users or groups. For more information about configuring SACLs, see “Setting Service Access Control Lists (SACLs)” on page 183.
- You can configure firewall rules that prevent Windows connections from unintended sources. For more information, see “Creating Firewall Service Rules” on page 216.

From the command line:

```
# Securely configure Windows file sharing service
sudo serveradmin settings smb:wins support = no
sudo serveradmin settings smb:domain master = no
sudo serveradmin settings smb:map to guest = "Never"
sudo serveradmin settings smb:auth methods = "odsam"
sudo serveradmin settings smb:ntlm auth = "no"
sudo serveradmin settings smb:max smbd processes = 1000
sudo serveradmin settings smb:log level = 1
sudo serveradmin settings smb:preferred master = no
sudo serveradmin settings smb:os level = 65
```

Configuring Share Points

A share point is a hard disk (or hard disk partition), disc media, or folder that contains files you want users to share. You can use share points to host home folders.

You can use Server Admin to set up share points and then use the share points to host local home folders. Or you can mount the share point so it hosts network home folders.

Using network home folders stored on a share point is inherently less secure than using local home folders. An intruder can access your network home folder through an insecure network connection.

Make sure that share points on local system drives are configured to grant access to only specific users or groups, and are not open to everyone. Removing open share points prevents unwanted access to your computer and prevents your computer from being used to maliciously access additional computers on the network. Do not share files unnecessarily.

Disabling Share Points

Disable unused share points and sharing protocols. Enabled share points and sharing protocols can provide an avenue of attack for intruders.

If you disable all share points using a specific sharing protocol, you should also disable that protocol.

To disable a share point:

- 1 Open Server Admin and connect to the server.
- 2 Click the file sharing protocol in the Computers & Services list.
- 3 Click Share Points and select the share point from the list.
- 4 Click Share Point below the list.
- 5 Click Protocol Options.
- 6 Disable the following sharing options:
 - Click AFP and deselect "Share this item using AFP."
 - Click SMB and deselect "Share this item using SMB."
 - Click FTP and deselect "Share this item using FTP."
 - Click NFS and deselect "Export this item and its contents to"
- 7 Click OK.
- 8 Click Save.

Restricting Access to a Share Point

Before enabling a share point, restrict the access permissions for the folder that will act as the share point and only allow users who must use the share point to access it.

You can then use Server Admin's File Sharing pane to set POSIX and ACL permissions to restrict share points to only being accessible by specific users. You can use a combination of the two permission types to customize accessibility for your users.

You can also use Workgroup Manager's effective permissions inspector to determine the permissions a user is granted.

WARNING: Carefully set access permissions. Incorrectly set access permissions can prevent legitimate users from accessing folders and files, or they can allow malicious users to access folders and files.

To restrict access to a share point:

- 1 Open Server Admin and connect to the server.
- 2 Click the file sharing protocol in the Computers & Services list.
- 3 Click Share Points and select the share point from the list.

- 4 Click Permissions below the list.
- 5 To set the owner or group of the shared item, enter names or drag names from the Users and Groups drawer to the owner or group records in the permissions table. The owner and group records are listed under the POSIX heading. The owner record has the single user icon. The group record has the group icon.

To open the drawer, click the Add (+) button. If you don't see a recently created user or group, click the Refresh button.

Owner and group names can also be edited by double-clicking a permissions record and dragging into or typing in the User/Group field in the window that appears.

Note: To change the autorefresh interval, choose Server Admin > Preferences and change the value of the "Auto-refresh status every" field.

Make sure you understand the implications of changing a folder's owner and group. For more information, see "Setting POSIX Permissions" on page 141.
- 6 To change the permissions for Owner, Group, and Others, use the Permission pop-up menu in the related row of the permissions table.

Others is any user that logs in to the file server who is not the owner and does not belong to the group.

If you're configuring a home folder's permissions, give the owner Read & Write privileges, but reduce group and everyone privileges to None.

The default for home folders is that the staff group and everyone have read privileges. All accounts are also members of the staff group. These two privileges allow everyone to view the contents of the home folder. If you want someone other than the owner to view the contents of the home folder, replace staff with that account.
- 7 Click Save.

The new share point is shared using AFP, SMB, and FTP, but not NFS.

To set ACL permissions on a share point or a folder:

 - 1 Open Server Admin and connect to the server.
 - 2 Click the file sharing protocol in the Computers & Services list.
 - 3 Click Share Points and select the share point from the list.
 - 4 Click Permissions below the list.
 - 5 Open the Users and Groups drawer by clicking the Add (+) button.
 - 6 Drag groups and users from the drawer into the ACL Permissions list to create ACEs.

By default, each new ACE gives the user or group full read and inheritance permissions.

The first entry in the list takes precedence over the second, which takes precedence over the third, and so on. For example, if the first entry denies a user the right to edit a file, other ACEs that allow the same user editing permissions are ignored. In addition, the ACEs in the ACL take precedence over standard permissions.

- 7 In the Access Control List, select the ACE.
- 8 Click the Edit (/) button.
- 9 From the Permission Type pop-up menu, choose "Allow" or "Deny."
- 10 In the Permissions list, select permissions.

If you chose Custom from the Permission pop-up menu, click the disclosure triangles to display specific attributes. Choose Allow or Deny from the Permission Type pop-up menu. Select specific permissions and click OK.

You can further grant or deny specific permissions that you cannot specify through POSIX permissions. For example, you can allow a user to list folder contents but disallow that user from reading file attributes.

- 11 Click Save.

AFP Share Points

If you supply network home folders, use AFP because it provides authentication-level access security. A user must log in with a valid user name and password to access files.

You can also enable AFP using an SSH-secured tunnel for file sharing. This tunnel prevents intruders from intercepting your communication with an AFP share point. You cannot enable SSH-secured tunnels for AFP share points that host home folders.

For more information, see "Configuring AFP File Sharing Service" on page 258.

SMB Share Points

Do not use SMB unless you're hosting a share point specifically for Windows users. You can set up a share point for SMB access only, so that Windows users have a network location for files that can't be used on other platforms.

Like AFP, SMB also requires authenticating with a valid user name and password to access files. However, there are well-known risks associated with SMB. For example, SMB uses NTLMv1 and NTLMv2 encryption, which are weak password hashing schemes.

For more information, see "Configuring SMB File Sharing Service" on page 263.

FTP Share Points

You cannot use FTP share points to host home folders and you should only enable FTP share points if you require anonymous access.

Files are transferred from FTP share points unencrypted over the network. Transferring files over FTP does not guarantee confidentiality or file integrity.

If you need to use FTP for file transfers, consider using the SSH service instead. The `sftp` command, part of the SSH suite of tools, provides an FTP-like experience for users while providing a more secure setting. For more information, see the `sftp` man page.

For more information about setting up FTP share points, see “Configuring FTP File Sharing Service” on page 259.

NFS Share Points

NFS file access is not based on user authentication (entering a user name and password). It is based on the user ID and the client IP address. As such, NFS share points without the use of Kerberos don’t have the same level of security as AFP and SMB, which require user authentication to gain access to a share point’s contents.

If you have NFS clients, consider setting up a share point to be used only by NFS users, or configure NFS with Kerberos. NFS doesn’t support SACLs.

Use NFS only if you must provide home folders for a large number of users who use UNIX workstations. Use Server Admin to restrict access to an NFS share point, so that only required computers can access it.

To restrict access to an NFS share point:

- 1 Open Server Admin and connect to the server.
- 2 Click the file sharing protocol in the Computers & Services list.
- 3 Click Share Points and select the share point from the list.
- 4 Click Share Point below the list.
- 5 Click Protocol Options.
- 6 Click NFS.
- 7 If only a few computers need access to the share point, select “Export this item and its contents to” and choose Client List from the pop-up menu.

To add a client, click Add (+) and enter the IP address of the client computer.

Add only those client computers that require access to the share point.

- 8 If every computer in a subnet requires access to the share point, select “Export this item and its contents to” and choose Subnet from the pop-up menu.

In the Subnet address field, enter the subnet address. In the Subnet mask field, enter the subnet mask.

- 9 From the Mapping pop-up menu, choose “All to nobody.”
A user with “nobody” privileges has “Others” POSIX permissions.
- 10 From the Minimum Security pop-up menu, set the level of authentication:
Choose “Standard” if you don’t want to set a level of authentication.
Choose “Any” if you want NFS to accept any method authentication.
Choose “Kerberos v5” if you want NFS to only accept Kerberos authentication.
Choose “Kerberos v5 with data integrity” if you want NFS to accept Kerberos authentication and validate the data (checksum) during transmission.
Choose “Kerberos v5 with data integrity and privacy” to have NFS accept Kerberos authentication, to validate using the checksum, and to encrypt data during transmission.
- 11 Select “Read-only.”
- 12 Click Save.

Use this chapter to learn how to secure web service.

Web service provides an easy method of accessing data from anywhere in the world.

However, this access is often attacked due to its weakness on other platforms.

Snow Leopard Server provides many configuration options to protect web service.

Web service is based on Apache, an open source HTTP web server. A web server responds to requests for HTML webpages stored on your site. Open source software gives you the capability to view and change the source code to make changes and improvements. This has led to Apache's widespread use, making it one of the most popular web servers on the Internet today.

Web administrators can use Server Admin to administer web service without knowing about advanced settings or configuration files. Web administrators proficient with Apache can also administer web technologies using Apache's advanced features.

Because web service in Snow Leopard Server is based on Apache, you add advanced features with plug-in modules. Apache modules let you add support for Simple Object Access Protocol (SOAP), Java, and CGI languages such as Python.

For more information about the Apache project, see www.apache.org. The Center for Internet Security (CIS) at www.cisecurity.org provides an Apache Benchmark and Scoring tool. CIS Benchmarks enumerate security configuration settings and actions that harden your computer.

For more information about configuring web service, see *Web Technologies Administration*.

Disabling Web Service

If the system is not intended to be a web server, disable web server software.

Secure web administration demands scrutiny of configuration settings. Use SSL encryption to encrypt sensitive web traffic.

If the system is not a web server, disable web services using the Server Admin tool.

Disabling the service prevents potential vulnerabilities on your computer. Web service is disabled by default, but verification is recommended.

To disable web service:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Stop Web.
- 4 Click Save.

From the command line:

```
# -----
# Securing Web Service
# -----  
  
# Disable web service:  
sudo serveradmin stop web
```

Managing Web Modules

If your system does not require active web modules, disable them. Web modules (sometimes called plug-ins) consist of web components that add functionality to web service. Using unnecessary modules creates potential security risks when the web service is running.

Many types of web modules are available for use with web service. Verify that each module used is required and that you understand the impact it has to security when web service is running.

Important: When disabling web modules, make sure the module is not needed by another web service you are running. If you disable a web module that another web service is dependent on, that web service might not work.

To disable web modules:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Settings, then click Modules.
- 4 Deselect all modules except for the modules your site requires.
- 5 Click Save.

Disabling Web Options

Enabled web options can be a security risk if you don't understand the impact the module has to security when a web service is running.

Disable the following web modules unless they are specifically required for a web service:

- **Folder Listing:** Displays a list of folders when users specify the URL and no default webpage (such as index.html) is present. Instead of viewing a default webpage, the server shows a list of the web folder's contents. Folder listings appear only if no default document is found.
- **WebDAV:** Turns on Web-based Distributed Authoring and Versioning (WebDAV), which allows users to make changes to websites while the sites are running. If you enable WebDAV you must also assign access privileges for the sites and for the web folders.
- **CGI Execution:** Permits Common Gateway Interface (CGI) programs or scripts to run on your web server. CGI programs or scripts define how a web server interacts with external content-generating programs.
- **Server Side Includes (SSI):** Permits SSI directives placed in webpages to be evaluated on the server while the website is active. You can add dynamically generated content to your webpages while the files are being viewed by users.
- **Allow All Overrides:** Instructs web service to look for additional configuration files inside the web folder for each request.
- **Spotlight Searching:** Allows web browsers to search the content of your website.

To disable web options:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services lists.
- 3 Click Sites, then select the website in the list.
- 4 Click Options below the websites list.
- 5 Deselect Folder Listing, WebDAV, CGI Execution, Server Side Includes (SSI), and Allow All Overrides unless they are required.

From the command line:

```
# Disable web options:  
sudo serveradmin settings web:Modules:_array_id:authz_host_module:enabled =  
    no  
sudo serveradmin settings web:Modules:_array_id:dav_module:enabled = no  
sudo serveradmin settings web:Modules:_array_id:dav_fs_module:enabled = no  
sudo serveradmin settings  
    web:Modules:_array_id:apple_spotlight_module:enabled = no  
sudo serveradmin settings web:Sites:_array_id:$SITE:SpotlightIndexing = no  
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/  
    Library/WebServer/Documents:AllowOverride = "None"  
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/  
    Library/WebServer/Documents:IfModule:_array_id:mod_dav.c:DAV = no  
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/  
    Library/WebServer/Documents:Options:Includes = no  
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/  
    Library/WebServer/Documents:Options:ExecCGI = no  
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/  
    Library/WebServer/Documents:Options:Indexes = no  
sudo serveradmin settings  
    web:Sites:_array_id:default_default:SpotlightIndexing = no
```

Using Realms to Control Access

You can use realms to control access and provide security to locations or folders in a website. Realms are locations at the URL or files in the folder that users can view.

If WebDAV is enabled, users with authoring privileges can also change content in the realm. You set up the realms and specify the users and groups that have access to them.

When an assigned user or group possesses fewer permissions than the permissions assigned to user Everyone, that user or group is deleted upon a refresh. This happens because the access assigned to Everyone preempts the access assigned to specific users or groups with fewer permissions than those possessed by Everyone. The greater permissions always take precedence.

Consequently, the list of assigned users and groups with fewer permissions are not saved in the Realms pane upon refresh if their permissions are determined to be preempted by the permissions assigned to Everyone. After the refresh, the names are no longer listed in the list on the right in the Realms pane. Also, for a brief period of time, user Everyone will switch its displayed name to “no-user.”

To use a realm to control website access:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites, then select the website in the list.
- 4 Below the websites list, click Realms.
- 5 Click the Add (+) button to create a realm.

The realm is the part of the website users can access.

- 6 In the Realm Name field, enter the realm name.

This is the name users see when they log in to the website.

- 7 From the Authentication pop-up menu, choose a method of authentication:
 - **Basic authentication** is on by default. Do not use basic authentication for sensitive data. It sends your password to the server unencrypted.
 - **Digest authentication** is more secure than basic authentication because it uses an encrypted hash of your password.
 - **Kerberos authentication** is the most secure because it implements server certificates to authenticate. If you want Kerberos authentication for the realm, join the server to a Kerberos domain.
- 8 Enter the realm location or folder you are restricting access to:

- a Choose Location from the pop-up menu and enter a URL to the location in the website that you want to restrict access to.
- b Choose Folder from the pop-up menu and enter the path to the folder that you want to restrict access to.

You can also click the Browse button to locate the folder you want to use.

- 9 Click OK.

- 10 Select the new realm and click Add (+) to open the Users & Groups panel.

To switch between the Users list and the Groups list, click Users or Groups in the panel.

Use the Realms pane to delete a user or group by selecting the name and clicking the Delete (-) button.

- 11 To add users or groups to a realm, drag users to the list on the right in the Realms pane.

When users or members of a group you've added to the realm connect to the site, they must supply their user name and password.

- 12 Limit realm access to specified users and groups by setting the following permissions using the up and down arrows in the Permissions column.
 - **Browse Only:** Permits users or groups to browse the website.
 - **Browse and Read WebDAV:** Permits users or groups to browse the website and also read the website files using WebDAV.
 - **Browse and Read/Write WebDAV:** Permits users or groups to browse the website and also read and write to website files using WebDAV.
 - **None:** Prevents users or groups from using permissions.
- 13 Click Save.

Enabling Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) provides security for a site and its users by authenticating the server, encrypting information, and maintaining message integrity.

SSL is a per-site setting that lets you send encrypted, authenticated information across the Internet. For example, if you want to permit credit card transactions through a website, you can protect the information that's passed to and from that site.

The SSL layer is below application protocols (for example, HTTP) and above TCP/IP. This means that when SSL is operating on the server and on the client computer, information is encrypted before being sent.

The Apache web server in Snow Leopard Server uses a public key-private key combination to protect information. A browser encrypts information using a public key provided by the server and only the server has a private key that can decrypt that information.

The web server supports SSLv2, SSLv3, and TLSv1. More information about these protocol versions is available at www.modssl.org.

When SSL is implemented on a server, a browser connects to it using the https prefix in the URL, rather than http. The "s" indicates that the server is secure.

When a browser initiates a connection to an SSL-protected server, it connects to a specific port (443) and sends a message that describes the encryption ciphers it recognizes. The server responds with its strongest cipher, and the browser and server then continue exchanging messages until the server determines the strongest cipher that it and the browser can recognize.

The server then sends its certificate (an ISO X.509 certificate) to the browser. This certificate identifies the server and uses it to create an encryption key for the browser to use. At this point a secure connection is established and the browser and server can exchange encrypted information.

Before you can enable SSL protection for a website, you must obtain the proper certificates. For detailed information about certificates and their management, see *Advanced Server Administration*.

To set up SSL for a website:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites, then select the website in the list.
- 4 Click Security below the websites list.
- 5 In the Security pane, select Enable Secure Sockets Layer (SSL).

When you turn on SSL, a message appears, noting that the port is changed to 443.

- 6 In the Certificate pop-up menu, choose the certificate you want.

If the certificate is protected by a passphrase, the name of the certificate must match the virtual host name. If the names don't match, web service won't restart.

- 7 If you choose Custom Configuration or want to edit a certificate, you might need to do the following:

- a Click the Edit (/) button and supply the information in each field for the certificate.
- b If you received a ca.crt file from the CA, click the Edit (/) button and paste the text from the ca.crt file in the Certificate Authority File field.

Note: The ca.crt file might be required but might not be sent directly to you. This file must be available on the website of the CA.

- c In the Private Key Passphrase field, enter a passphrase and click OK.

- 8 In the "SSL Log File" field, enter the pathname for the folder where you want to keep the SSL log.

You can also use the Browse button to navigate to the folder.

- 9 Click Save.

- 10 Confirm that you want to restart web service.

Server Admin lets you enable SSL with or without saving the SSL passphrase. If you did not save the passphrase with the SSL certificate data, the server prompts you for the passphrase upon restart but won't accept manually entered passphrases.

Use the Security pane for the site in Server Admin to save the passphrase with the SSL certificate data. For more information, see "Using a Passphrase with SSL Certificates" on page 278.

Using a Passphrase with SSL Certificates

If you manage SSL certificates using Server Admin and you use a passphrase for certificates, Server Admin ensures that the passphrase is stored in the system keychain.

When a website is configured to use the certificate and that web server is started, the `getsslpassphrase(8)` utility extracts the passphrase from the system keychain and passes it to the web server, as long as the certificate name matches the virtual host name.

If you do not want to rely on this mechanism, you can have the Apache web server prompt you for the passphrase when you start or restart it. Use the `sudo serveradmin` command-line tool to configure this.

To configure Apache to prompt you for a passphrase when it starts:

- 1 Open Terminal and enter the following command.

```
sudo serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL  
PassPhraseDialog= builtin
```

- 2 Start Apache with the command:

```
sudo serveradmin start web
```

- 3 When prompted, enter the certificate passphrase.

From the command line:

```
#  
# Configure Apache to prompt you for a passphrase when it starts.  
#-----  
sudo serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL  
PassPhraseDialog= builtin
```

Viewing Web Service Logs

Use Server Admin to view the error and access logs for web service, if you have enabled them. web service in Snow Leopard Server uses the standard Apache log format, so you can also use a third-party log analysis tool to interpret the log data.

To view logs:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Logs, then choose between an access or error log by selecting the log from the list of logs.

To search for specific entries, use the Filter field in the lower right.

From the command line:

```
#  
# View logs.  
-----  
sudo tail /var/log/apache2/access_log
```

Securing WebDAV

Web service includes support for Web-based Distributed Authoring and Versioning, known as WebDAV. With WebDAV capability, your users can check out webpages, make changes, and then check the pages back in while the site is running. In addition, the WebDAV command set is rich enough that client computers with Snow Leopard installed can use a WebDAV-enabled web server as if it were a file server.

Sharing files over a network opens your computers to a host of vulnerabilities. To reduce the security risk when using WebDAV, assign access privileges for the sites and for the web folders.

To securely configure WebDAV for a site:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites, then select the website in the list.
- 4 Click Options below the websites list.
- 5 Select the WebDAV checkbox.

This option turns WebDAV on, allowing users to make changes to websites while the sites are running. If you enable WebDAV, you must also assign access privileges for the sites and web folders.

Note: If you turned off the WebDAV module in the Modules pane of Server Admin, you must turn it on again before WebDAV takes effect for a site. This is true even if the WebDAV option is selected in the Options pane for the site. For more about enabling modules, see “Managing Web Modules” on page 272.

- 6 Click Save.

After WebDAV is turned on, you can use realms to control access to the website. For more information about configuring realms, see “Using Realms to Control Access” on page 274.

Securing Blog Services

A blog is like a diary or journal, with entries that are arranged in the order they were created in. On the other hand, a wiki contains shared content that doesn't appear in chronological order. The type of information you want to put on your site helps determine whether it appears in a wiki or in a blog.

By default, blogs are disabled when you start web service. Blogs can open your computers to a host of vulnerabilities. If blogs are not required, disable them.

Disabling Blog Services

If you do not need blog services, disable them.

To disable blog service:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites.
- 4 In the Sites list, click the site where you want blog service disabled.
- 5 Click Web Services.
- 6 In the Services for Groups section, deselect the "Wiki and blog" checkbox.
- 7 Click Save.

From the command line:

```
#  
# Disable blog service.  
#-----  
sudo serveradmin settings web:Sites:_array_id:$SITE:weblog = no
```

Securely Configuring Blog Services

You can enable user and group blog service on your website. Snow Leopard Server includes a group wiki and a group blog. These are enabled together. Group blogs let users in a group access and post entries to the same blog.

Users can also publish their own personal blog using web services associated with their server account. This gives users the ability to maintain personal blogs on their own user pages.

To set up blog service:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Sites.

- 4 In the Sites list, click the site where you want blog service enabled.

To maximize the security of user interactions with the server hosting blogs, have users access blogs through a site that has SSL enabled.
- 5 Click Web Services.
- 6 In the Services for Groups section, select the “Wiki and blog” checkbox.
- 7 Click Settings.
- 8 Click Web Services.
- 9 Click blogs.
- 10 From the default Wiki and Blog Theme pop-up menu, choose a theme.

A theme controls the appearance of a blog. Themes determine the color, size, location, and other attributes of blog elements. Each theme is implemented using a style sheet.

The default theme is used when a blog is created, but blog owners can change the theme. The default theme also controls the appearance of the blog’s front page.
- 11 Identify a blog folder, used to store blog files.

By default, blog files are stored in /Library/Collaboration on the computer hosting blog service. You can click Choose to select a different folder, such as a folder on a RAID device or on another computer.
- 12 Click Save.
- 13 Make sure the blog server’s Open Directory search path includes directories where users and group members you want to support with blog service are defined.

The *Open Directory Administration* guide explains how to set up search paths. Any user or group member defined in the Open Directory search path can create and access blogs on the server unless you deny them access to blog service.

Securing Tomcat

You use Server Admin or Terminal to disable Tomcat if you don’t need it.

To stop Tomcat using Server Admin:

- 1 Open Server Admin and connect to the server.
- 2 Select Web in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 Deselect the Enable Tomcat checkbox.
- 5 Click Save.

From the command line:

```
# -----  
# Securing Tomcat  
# -----  
  
# Stop Tomcat using Server Admin:  
sudo /Library/Tomcat/bin/startup.sh stop
```

Securing MySQL

MySQL provides a relational database management solution for your web server. With this open source software, you can link data in tables or databases and provide the information on your website.

Disabling MySQL Service

If you do not need to run MySQL service, disable it in Server Admin.

To turn MySQL service on:

- 1 Open Server Admin and connect to the server.
- 2 Select MySQL in the Computers & Services list.
- 3 Click Stop MySQL.

From the command line:

```
# -----  
# Securing MySQL  
# -----  
  
# Turn MySQL service off  
sudo serveradmin stop mysql
```

Setting Up MySQL Service

Use MySQL service Settings in Server Admin to specify the database location, to enable network connections, and to set the MySQL root password.

To configure MySQL service settings:

- 1 Open Server Admin and connect to the server.
- 2 Select MySQL in the Computers & Services list.
- 3 Click Settings.

- 4** To prevent user to access MySQL service deselect the “Allow network connections” checkbox.
This prohibits user access to database information through the web server.
- 5** In the Database location field enter the path to the location of your database.
You can also click the Choose button and browse for the folder you want to use.
- 6** Click Save.

From the command line:

```
#  
# Configure MySQL service settings.  
#-----  
sudo serveradmin settings mysql:allowNetwork = no
```

Viewing MySQL Service and Admin Logs

MySQL service keeps two types of logs, a MySQL service log and MySQL admin logs:

- The MySQL service log records the time of events such as when MySQL service is started and stopped.
- The MySQL admin log records information such as when clients connect or disconnect and each SQL statement received from clients. This log is located at / Library/Logs/MySQL.log.

You can view MySQL service logs using Server Admin.

To view MySQL service logs:

- 1** Open Server Admin and connect to the server.
- 2** Select MySQL in the Computers & Services list.
- 3** Click Logs.

Use the Filter field to search for specific entries.

From the command line:

```
#  
# View MySQL service logs.  
# -----  
sudo tail /Library/Logs/MySQL.log
```

Use this chapter to learn how to secure Client Configuration Management services.

Securely configuring client configuration management helps standardize the clients across your network and provides a secure deployment.

By managing preferences for users, workgroups, computers, and computer groups, you can customize the user's experience and restrict user access to only the applications and network resources you choose.

To manage preferences, use the Preferences pane in Workgroup Manager.

Properly set managed preferences help deter users from performing malicious activities. They can also help prevent users from accidentally misusing their computer.

Managing Applications Preferences

Use Applications preferences to allow or restrict user access to applications.

Computers identify applications using one of two methods: digital signatures (used in Leopard or later), and bundle IDs (used in Tiger or earlier, but can be used in Snow Leopard or later).

Digital signatures are much more secure because clever users can manipulate bundle IDs. Workgroup Manager supports both methods.

Use the Applications pane to work with digital signatures. Use the Legacy pane to work with bundle IDs.

Application restrictions depend on which pane you're managing and the version of Mac OS X run by client computers:

- If you manage the Applications pane and your users run Snow Leopard or later, Applications settings take effect and Legacy settings are ignored.
- If you don't manage the Applications pane, Legacy settings take effect for any version of Mac OS X.
- If your users run Tiger or earlier, only Legacy settings take effect.

You can also use settings in Applications preferences to allow only specific widgets in Dashboard or to disable Front Row.

The table below describes the settings in each Applications pane.

Applications preference pane	What you can control
Applications	Access to specific applications and paths to applications using digital signatures (for users of Snow Leopard or later)
Widgets	Allowed Dashboard widgets for users of Snow Leopard
Front Row	Whether Front Row is allowed
Legacy	Access to specific applications and paths to applications using bundle IDs (primarily for users of Tiger or earlier)

Controlling User Access to Applications and Folders

You can use Workgroup Manager to prevent users from launching unapproved applications or applications located in unapproved folders.

In Tiger or earlier, applications were identified by their bundle IDs. If users have Snow Leopard or later installed, you can use digital signatures to identify applications. Digital signatures are much more difficult to circumvent than a bundle ID.

Workgroup Manager can sign applications that aren't already signed. When signing an application, you can embed a signature or you can store a detached signature separately from the application.

Embedding a signature has several performance benefits over a detached signature, but with signature embedding you must make sure every computer has the same signed application. For applications run from a CD, DVD, or other read-only media, you must use detached signatures.

Workgroup Manager uses the following icons to denote the kind of signature associated with an application.

Icon	Indicates the application has this type of signature
(no icon)	Embedded signature
	Detached signature
	No signature

Applications that include helper applications are denoted by a disclosure triangle. When you click the disclosure triangle, you'll see a list of helper applications. By default, these helper applications are allowed to open.

You can disable individual helper applications, but the application might behave erratically if it requires the helper applications.

To allow or prevent users from launching an application, add the application or application path to one of three lists:

- **Always allow these applications.** Add applications that should always be allowed, regardless of their inclusion in other lists. You can sign applications added to this list. Do not add unsigned applications to this list because they allow users to disguise unapproved applications as approved applications.
- **Disallow applications within these folders.** Add applications and folders containing applications you want to prevent users from opening. All applications in the subfolders of a disallowed folder are also disallowed. Disallowing a folder in an application package can cause the application to behave erratically or fail to load.
- **Allow applications within these folders.** Add applications and folders containing applications you want to allow. All applications in the subfolders of an allowed folder are also allowed. Unlike applications in the "Always allow these applications" list, applications listed here are not allowed if they or their paths are listed in the "Disallow applications within these folders" list.

If an application or its folder doesn't appear in these lists, the user can't open the application.

Some applications don't fully support signatures. To make sure a signed application is restricted, make a copy of the application, sign it, and move it to a location in the "Disallow applications within these folders" list. When you try to open the application on a managed computer, it should open because the signature is valid.

Next, void the signed application's signature by copying a file into its application package. Now when you try to open the application on a managed computer, it should not open because the signature is void and the application is in a disallowed folder.

To manage Applications preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Applications and then click the Applications tab.
- 5 Set the management setting to Always.
- 6 Select “Restrict which applications are allowed to launch.”
- 7 Click the Applications tab (in the Applications pane), click the Add (+) button, choose an application you want to always allow, and then click Add.

When you allow an application, you also allow all helper applications included with that application. You can deselect helper applications to disallow them.

- 8 If you’re asked to sign the application, click Sign; if you’re asked to authenticate, authenticate as a local administrator.

To add the application to the list as an unsigned application, click Don’t Sign.

When you sign the application, Workgroup Manager tries to embed the signature. If you don’t have write access to the application, Workgroup Manager creates a detached signature.

- 9 Click the Folders tab, click the Add (+) button next to “Disallow applications within these folders,” and then choose folders containing applications you want to prevent users from launching.
- 10 Click the Add (+) button next to the “Allow applications within these folders” field and choose folders containing applications you want to allow.
Disallowing folders takes precedence over allowing them. If you allow a folder that is a subfolder of a disallowed folder, the subfolder is still disallowed.
- 11 Click Apply Now.

Allowing Specific Dashboard Widgets

If your users have Snow Leopard or later installed, you can prevent them from opening unapproved Dashboard widgets by creating a list of approved widgets (which can include widgets included with Snow Leopard and third-party widgets). To approve third-party widgets, you must be able to access them from your server.

The Dashboard widgets included with Snow Leopard Server can be trusted. However, users can install third-party Dashboard widgets without authenticating. To protect systems against unauthorized use, allow users to use only trusted third-party Dashboard widgets.

Note: Because code signing is not supported, users can bypass restrictions to Dashboard widgets. Therefore, implement a mechanism to regularly check available Dashboard widgets to ensure policy compliance.

To allow specific Dashboard widgets:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Applications and then click Widgets.
- 5 Set the management setting to Always.
- 6 Select "Allow only the following Dashboard widgets to run."
- 7 To allow specific widgets, click the Add (+) button, select the widget's .wdgt file, and then click Add.

The widgets included with Snow Leopard are in /Library/Widgets.

- 8 To prevent users from opening specific widgets, select the widget and click the Remove (-) button.
- 9 Click Apply Now.

Disabling Front Row

With Workgroup Manager, you can disable Front Row.

To disable Front Row:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Applications and then click Front Row.
- 5 Set the management setting to Always.
- 6 Deselect Allow Front Row.
- 7 Click Apply Now.

From the command line:

```
# Securing Client Configuration Management Services
# =====
# If the intended target is a client system, the target for the dscl
# commands should be "/LDAPv3/127.0.0.1". If the management target is the
# server itself, the target should be ..

# Disable Front Row:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.frontrow
    PreventActivation always -bool 1
```

Allowing Legacy Users to Open Applications and Folders

To control user access to applications in Tiger or earlier, you:

- Provide access to a set of approved applications that users can open
- Prevent users from opening a set of unapproved applications

You can also set options to further control user access to applications.

When users have access to local volumes, they can access applications on the computer's local hard disk. If you don't want to allow this, disable local volume access.

Applications use helper applications for tasks they can't complete independently. For example, if a user tries to open a web link in a mail message, the mail application might need to open a web browser to display the webpage.

Disallowing helper applications improves security because an application can designate any other application as a helper application. However, you might want to include common helper applications in the approved applications list. This avoids problems such as users being unable to open and view mail content or attached files.

Occasionally, applications or the operating system might require the use of UNIX tools, such as QuickTime Image Converter. These tools can't be accessed directly, and generally operate in the background without the user's knowledge. If you disallow access to UNIX tools, some applications might not work.

Allowing UNIX tools enhances application compatibility and efficient operation, but can decrease security.

If you don't manage Applications settings for computers running Snow Leopard or later, Legacy settings are used.

To set up a list of accessible applications:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Applications and then click Legacy.
- 5 Set the management setting to Always.
- 6 Select “User can only open these applications” or “User can open all applications except these.”
- 7 Add items to or remove items from the list.
To select multiple items, hold down the Command key.
- 8 To allow access to applications stored on the user’s local hard disk, select “User can also open all applications on local volumes.”
- 9 To allow helper applications, select “Allow approved applications to launch non-approved applications.”
- 10 To allow use of UNIX tools, select “Allow UNIX tools to run.”
- 11 Click Apply Now.

From the command line:

```
# Setting up a list of accessible applications
# -----
# Allow access to applications stored on the user's local hard disk:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess OpenItemsInternalDrive always -bool 1

# Allow helper applications:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess ApprovedAppLaunchesOthers always -bool 1

# Allow UNIX tools:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess AllowUnbundledApps always -bool 1
```

Managing Dock Preferences

You can customize the user's Dock to display specific applications. This helps you guide the user toward using recommended applications.

You can also add documents and folders to the Dock. Adding specific, required network folders to the Dock helps prevent the user from navigating through your network hierarchy. This also helps prevent them from misusing the server.

To manage Dock preferences:

- 1 In Workgroup Manager, click Preferences.

- 2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

- 3 Select users, groups, computers, or computer groups.

- 4 Click Dock and then click Dock Display.

- 5 Set the management setting to Once or Always.

- 6 Drag the Dock Size slider to make the Dock smaller or larger.

- 7 If you want items in the Dock to be magnified when a user moves the pointer over them, select Magnification and then adjust the slider.

Magnification is useful if you have many items in the Dock.

- 8 From the "Position on screen" radio buttons, select whether to place the Dock on the left, right, or bottom of the desktop.

- 9 From the "Minimize using" pop-up menu, choose a minimizing effect.

- 10 If you don't want to use animated icons in the Dock when an application opens, deselect "Animate opening applications."

- 11 If you don't want the Dock to be visible all the time, select "Automatically hide and show the Dock."

When the user moves the pointer to the edge of the screen where the Dock is located, the Dock appears.

- 12 Click Apply Now.

From the command line:

```
# Managing Dock Preferences
# -----
# Set Dock hiding
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock autohide-
    immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock autohide
    always -bool 1
```

Managing Energy Saver Preferences

Energy Saver preference settings help you save energy and battery power by managing wake, sleep, and restart timing for servers and client computers. You can only manage Energy Saver preferences for computer lists.

When client computers go to sleep, they become unmanaged. Do not enable sleep mode for client computers.

To manage Energy Saver preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select computers or computer groups.
- 4 Click Energy Saver and then click Desktop.
- 5 From the OS pop-up menu, choose Mac OS X and set the management setting to Always.
- 6 To adjust sleep settings, choose Sleep from the Settings pop-up menu and move the “Put the computer to sleep when it is inactive for” slider to Never.
- 7 From the OS pop-up menu, choose Snow Leopard Server and set the management setting to Always.
- 8 From the Settings pop-up menu, choose Sleep and move the “Put the computer to sleep when it is inactive for” slider to Never.
- 9 Click Portable.
- 10 From the Power Source pop-up menu, choose Adapter and set the management setting to Always.
- 11 From the Settings pop-up menu, choose Sleep and move the “Put the computer to sleep when it is inactive for” slider to Never.

- 12 From the Power Source pop-up menu, choose Battery and set the management setting to Always.
- 13 From the Settings pop-up menu, choose Sleep and move the “Put the computer to sleep when it is inactive for” slider to Never.
- 14 Click Schedule.
- 15 From the OS pop-up menu, choose Mac OS X and set the management setting to Always.
- 16 Deselect “Start up the computer.”
- 17 From the OS pop-up menu, choose Snow Leopard Server and set the management setting to Always.
- 18 Deselect “Start up the computer.”
- 19 Click Apply Now.

Managing Finder Preferences

You can control aspects of Finder menus and windows to improve or control workflow.

You can prevent users from burning media or from ejecting disks, and from connecting to remote servers. When used with Dock preferences, you can guide the user experience.

To manage Finder preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Overview.
- 5 Click Finder, click the Preferences tab, and then select Always.
- 6 Select “Use normal Finder.”

Simple Finder is best used for computers in kiosk situations.

Simple Finder removes the ability to use a Finder window to access applications or modify files. This limits users to accessing only what is in the Dock. If you enable Simple Finder, users cannot mount network volumes. With Simple Finder enabled, users cannot create folders or delete files.

- 7 Deselect “Hard disks,” “Removable media (such as CDs),” and “Connected servers.”

By deselecting these, you help prevent users from casually navigating through local and network file systems.

- 8 Select "Always show file extensions."

Important: Operating systems use file extensions as one method of identifying types of files and their associated applications. Using only file extensions to check the safety of incoming files leaves your system vulnerable to attacks by Trojans. A Trojan is a malicious application that uses common file extensions or icons to masquerade as a document or media file (such as a PDF, MP3, or JPEG).

For further explanation and guidance on handling mail attachments and content downloaded from the internet, see KBase Article 108009: Safety tips for handling email attachments and content downloaded from the Internet atdocs.info.apple.com/article.html?artnum=108009.

- 9 Click Commands and select Always.

- 10 Deselect Connect to Server, Go to iDisk, and Go to Folder.

Instead of allowing the user to choose which servers or folders to load, add approved servers.

- 11 Deselect Eject and Burn Disc.

Disallowing external media gives you more control.

- 12 Deselect Restart and Shut Down.

By disallowing restarting and shutting down client computers, you help ensure that your computers are available to other users.

- 13 Click Apply Now.

From the command line:

```
# Managing Finder Preferences
# -----
# Manage Finder preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    AppleShowAllExtensions-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitBurn always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitConnectTo always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitEject always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitGoToFolder always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitGoToDisk always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowHardDrivesOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowMountedServersOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowRemovableMediaOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
    AppleShowAllExtensions always -bool 1
```

Managing Login Preferences

Use Login preferences to set options for user login, to provide password hints, and to control the user's ability to restart and shut down the computer from the login window. You can also mount a group volume or set applications to open when a user logs in.

The table below summarizes what you can do with settings in each Login pane.

Login preference pane	What you can control
Window	<i>For computers and computer groups only:</i> The appearance of the login window such as the heading, message, which users are listed if the "List of users" is specified, and the ability to restart or shut down
Options	<i>For computers and computer groups only:</i> Login window options like enabling password hints, automatic login, console, fast user switching, inactivity logout, disabling of management, setting the computer name to match the computer record, and external account login
Access	<i>For computers and computer groups only:</i> Who can log in, if local users can use workgroup settings, and the combination and selection of workgroups

Login preference pane	What you can control
Scripts	<i>For computers and computer groups only:</i> A script to run during login or logout and whether to execute or disable the client computer's own LoginHook or LogoutHook scripts
Items	Access to the group volume, which applications open automatically for the user, and if users can add or remove login items

By managing script settings, you can help protect your users from malicious login or logout scripts that could be used to compromise their accounts integrity.

You can manage login window settings to make it more difficult for intruders to attempt to log in as legitimate users.

You can configure options to track malicious user actions.

To manage Login preferences:

1 In Workgroup Manager, click Preferences.

2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

3 Select user accounts.

To perform the steps involving applying scripts and login window settings, select computers or computer groups.

4 Click Overview and click Login.

5 Click Items and select Always.

Different login items settings are available depending on whether you're managing Once or Always. Like all managed preferences, you should use the Always setting to ensure that your settings stay in effect past the user's first login.

6 To load applications or to mount a group volume at startup, click Add to open a dialog where you can add an application or volume.

7 Add the applications required, including antivirus and file integrity checking applications required by your organization.

8 Deselect "Add network home share point."

Instead of automatically mounting share points, the user should mount share points as required.

9 Deselect "User may add and remove additional items" and "User may press Shift to keep items from opening."

Deselecting these options helps prevent the user from loading potentially malicious applications. It also helps ensure that the user cannot bypass loading applications required by your organization.

- 10 Click Scripts and select Always.
- 11 Unless your organization requires the use of specific login or logout scripts, deselect Login Script and Log-Out Script, and then deselect “Also execute the client computer’s LoginHook script,” and “Also execute the client computer’s LogoutHook script.”

To run login and logout scripts, the client’s computer must have a level of trust with the server. This level of trust is based on how secure the client’s connection is with the server. By requiring a level of trust, this ensures that the client computer does not run scripts from malicious servers.

For more information about how to enable the use of login and logout scripts, see the *User Management* guide.
- 12 Click Window and select Always.
- 13 Select “Login Window message” and enter help desk contact information in the adjacent field.

Do not enter information about the computer’s typical usage or who its users are.
- 14 In “Display Login Window as,” select “Name and password text fields.”

Requiring that users know their account names adds a layer of security and helps prevent intruders from compromising accounts with weak passwords.
- 15 Deselect “Show Restart button in the Login Window” and “Show Shut Down button in the Login Window.”

Preventing users from easily restarting or shutting down the computer helps ensure that the computer is available to all users.
- 16 Deselect “Show password hint after 3 attempts to enter a password.”

Password hints can help malicious users compromise accounts. If you enable this setting, set the password hint per user account to information for your organization’s help desk.
- 17 Deselect “Auto Login Client Setting.”

Enabling this setting allows users to enable automatic login through System Preferences. Automatic login bypasses all login window-based security mechanisms.
- 18 Deselect “Allow users to log in using ‘>console.’”

Enabling this setting allows the user to bypass the login window and use the Darwin console (command-line interface).
- 19 Click Options and select Always.
- 20 Deselect Enable Fast User Switching.

Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is actively using the computer.

- 21** Deselect “Log out users after # minutes of inactivity.”

If you select “Log out users after # minutes of inactivity,” enable password-protected screensavers in case a dialog prevents logging out.

- 22** Click Apply Now.

From the command line:

```
# Managing Login Preferences
#
# Manage login preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow LoginwindowText always -string
    "$LOGIN_WINDOW_MESSAGE"
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow mcx_UseLoginWindowText always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow RestartDisabled always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow ShutDownDisabled always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow SHOWFULLNAME always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow DisableConsoleAccess always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
    MultipleSessionEnabled always -bool 0
```

Managing Media Access Preferences

Media Access preferences let you control settings for, and access to, CDs, DVDs, the local hard disk, and external disks (for example, floppy disks and FireWire drives).

Disable unnecessary media. If users can access external media, it provides opportunities for performing malicious activities. For example, they can transfer malicious files from the media to the hard disk. Another example is if an intruder gains temporary access to the computer, he or she can quickly transfer confidential files to the media.

Carefully weigh the advantages and disadvantages of disabling media. For example, disabling external disks prevents you from using USB flash memory drives for storing keychains. For more information, see “Storing Credentials in Keychains” on page 88.

To manage Media Access preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Overview and click Media Access.
- 5 Select Always and click Disc Media.
- 6 Unless you must use disc media, deselect Allow for CDs & CD-ROMs, DVDs, and Recordable Discs.
To enable disc media, select both Allow and Require Authentication for that disc media.
- 7 Click Other Media.
- 8 Unless you must use media, deselect Allow for Internal Disks and External Disks.
If you must enable media, select Allow and Require Authentication for that disc media. Select Read-Only if you do not need to save files to that media.
- 9 Select "Eject all removable media at logout."
This helps prevent users from forgetting they have media inserted in the computer.
- 10 Click Apply Now.

Managing Mobility Preferences

You can use Mobility preferences to enable and configure mobile accounts for users during their next login.

If your computers have Snow Leopard or later, you can also encrypt the contents of the mobile account's portable home directory, restrict its size, choose its location, or set an expiration date on the account.

Mobile accounts include a network home folder and a local home folder. By having these two types of home folders, clients can take advantage of features available for local and network accounts. You can synchronize specific folders of these two home folders, creating a portable home directory.

Avoid using mobile accounts. When you access a mobile account from a client computer and create a portable home directory, you create a local home folder on that client computer. If you access the mobile account from many computers, creating portable home directories on each computer, your home folder's files are stored on several computers. This provides additional avenues of attack.

If you use mobile accounts, do not create portable home directories on computers that are physically insecure, or that you infrequently access. Enable FileVault on every computer where you create portable home directories. For more information about enabling FileVault, see “Securing Security Preferences” on page 122.

To manage Mobility preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select a user account, group account, computer, or computer group.
- 4 Click Overview.
- 5 Click Mobility, click Account Creation, and then click Creation.
- 6 Set the management setting to Always.
- 7 To disable mobile accounts, deselect “Create mobile account when user logs in to network account”; to enable mobile accounts, select this option.
- 8 Select “Require confirmation before creating a mobile account.”

If this is deselected, a portable home directory is created every time the user accesses a different computer.
- 9 Select “with syncing off.”
- 10 Click Rules, click Login & Logout Sync, and select Always.
- 11 In the “Sync at login and logout” list, click the Add (+) button and enter the paths of folders located in the user’s home folder.

Alternatively, click the browse (...) button to open a dialog where you can choose folders to add to the list and then add folders that do not contain confidential files.
- 12 In the “Skip items that match any of the following” list, click the Add (+) button and enter the paths of folders located in the user’s home folder.

Alternatively, click the browse (...) button to open a dialog where you can choose folders to add to the list and then add folders that contain confidential files.
- 13 Deselect “Merge with user’s settings.”

By deselecting this setting, the folders you synchronize replace those chosen by the user.
- 14 Click Background Sync. Select Always.
- 15 In the “Sync at login and logout” list, click the Add (+) button and enter the paths of folders located in the user’s home folder.

Alternatively, click the browse (...) button to open a dialog where you can choose folders to add to the list and then add folders that do not contain confidential files.

- 16 In the “Skip items that match any of the following” list, click the Add (+) button and enter the paths of folders located in the user’s home folder.

Alternatively, click the browse (...) button to open a dialog where you can choose folders to add to the list and then add folders that contain confidential files.
- 17 Deselect “Merge with user’s settings.”

By deselecting this setting, the folders you choose to synchronize replace those chosen by the user.
- 18 Click Apply Now.

Managing Network Preferences

Network preferences let you select and configure proxy servers that can be used by users and groups. You can also specify hosts and domains to bypass proxy settings.

Using proxy servers controlled by your organization can help improve security. You can also decrease the performance hit from using proxies if you selectively bypass trusted hosts and domains (like choosing local resources or trusted sites).

You can also disable Internet Sharing, Airport, or Bluetooth. Disabling these can improve security by removing avenues for attack.

To manage Network preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Overview.
- 5 Click Network and then click Proxies.
- 6 Set the management setting to Always.
- 7 Select a type of proxy server and enter the network address and port of a proxy server controlled by your organization.
- 8 If you select Automatic Proxy Configuration, enter the URL of your automatic proxy configuration (.pac) file.

- 9 In the “Bypass proxy settings for these Hosts & Domains” field, enter the addresses of the hosts and domains that you want users to connect to directly.

To enter multiple address, separate the subnet masks with new lines, spaces, semicolons, or commas. There are several ways to enter addresses:

 - A subdomain or fully qualified domain name (FQDN) of a target server, such as server1.apple.com or store.apple.com.
 - The specific IP address of a server, such as 192.168.2.1.
 - A domain name, such as apple.com. This bypasses apple.com, but not subdomains, such as store.apple.com.
 - An website, including subdomains, such as *.apple.com.
 - A subnet in Classless Inter-Domain Routing (CIDR) notation. For example, to add a subnet of IP addresses from 192.168.2.0 to 192.168.2.255, name that view 192.168.2.0/24. For a description of subnet masks and CIDR notation, see the *Network Services Administration* guide.
- 10 Deselect Use Passive FTP Mode (PASV).
- 11 Click Apply Now.

From the command line:

```
# Managing Network Preferences
#
# -----
# Manage network preferences:
sudo networksetup -setwebproxystate Ethernet on
sudo networksetup -setwebproxy Ethernet "http://$SERVER" 8008

sudo networksetup -setpassiveftp Ethernet on
```

Managing Parental Controls Preferences

Parental Controls preferences allow you to hide profanity in Dictionary, limit access to websites, or set time limits or other constraints on computer usage. To manage Parental Controls preferences, computers must have Snow Leopard or later.

Note: Parental control does not apply to directory users. It applies to only local users.

The table below describes Parental Controls settings.

Parental Controls preference pane	What you can control
Content Filtering	Whether profanity is allowed in Dictionary, and limitations on which websites users can view
Time Limits	How long and when users can log in to their accounts

Hiding Profanity in Dictionary

You can hide profane terms from the Dictionary application included with Snow Leopard or later. When you hide profane terms, entirely profane terms are removed from search results. If you search for a profane term that has an alternate nonprofane definition, Dictionary only displays the nonprofane definition.

To hide profanity in Dictionary:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Parental Controls and then click Content Filtering.
- 5 Set the management setting to Always.
- 6 Select "Hide profanity in Dictionary."
- 7 Click Apply Now.

From the command line:

```
# Managing Parental Control Preferences
#
# -----
# Hide profanity:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.Dictionary
    parentalControl always -bool 1
```

Preventing Access to Adult Websites

You can use Workgroup Manager to help prevent users from visiting adult websites. You can also block access to specific websites while allowing users to access other websites. You can allow or deny access to specific subfolders in the same website.

Instead of preventing access to specific websites, you can allow access only to specific websites. For more information, see "Allowing Access Only to Specific Websites" on page 304.

To prevent access to websites:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.

- 4** Click Parental Controls and then click Content Filtering.
 - 5** Set the management setting to Always.
 - 6** Select “Limit access to websites by” and choose “trying to limit access to adult websites.”
 - 7** To allow access to specific sites, click the Add (+) button next to the “Always allow sites at these URLs” list and then enter the URL of the site you want to allow.
 - 8** To block access to specific sites, click the Add (+) button next to the “Never allow sites at these URLs” list and then enter the URL of the site you want to block.
- To allow or block a site, including all content stored in its subfolders, enter the highest level URL of the site.
- For example, allowing “www.example.com” lets the user view all pages in www.example.com. However, blocking “www.example.com/banned/” prevents the user from viewing content stored in www.example.com/banned/, including all subfolders in /banned/, but it allows the user to view pages in www.example.com that are not in /banned/.
- 9** Click Apply Now.

Allowing Access Only to Specific Websites

You can use Workgroup Manager to allow access only to specific websites on computers with Snow Leopard or later.

If the user tries to visit a website that he or she is not allowed to access, the web browser loads a webpage that lists all sites the user is allowed to access.

To help direct users to allowed sites, the user’s bookmarks are replaced by websites you allow access to. The bookmarks created by allowing access to websites are called *managed bookmarks*.

If the user syncs bookmarks with MobileMe, the first time the user syncs he or she is asked if MobileMe should merge or replace its bookmarks with the managed bookmarks. If the user merges bookmarks, the MobileMe bookmarks will include the original MobileMe bookmarks and the managed bookmarks. If the user replaces bookmarks, the MobileMe bookmarks include only the managed bookmarks.

You can also use Workgroup Manager to block specific websites instead of blocking all websites. For more information, see “Preventing Access to Adult Websites” on page 303.

To allow access only to specific websites:

- 1** In Workgroup Manager, click Preferences.
- 2** Make sure the correct directory is selected and you are authenticated.

To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.

- 3** Select users, groups, computers, or computer groups.
- 4** Click Parental Controls and then click Content Filtering.
- 5** Set the management setting to Always.
- 6** Select “Limit access to websites by” and choose “allowing access to the following websites only.”
- 7** Use one of the following methods to add websites that you want to allow access to:
 - In Safari, open the site and then drag the icon from the address bar (of Safari) to the list.
 - In Safari, choose Bookmarks > Show All Bookmarks, then drag icons from the bookmark list to the list in Workgroup Manager.
 - If you have a .webloc file of the website you want to allow access to, drag the file into the list.
 - If you don’t have a .webloc file of the website you want to allow access to, click the Add (+) button and enter the URL of the website you want to allow.In the “Web site title” field, name the website. In the Address field, enter the highest level URL of the site.

For example, allowing “www.example.com” lets the user view all pages in www.example.com. Allowing “www.example.com/allowed/” lets the user view content stored in www.example.com/allowed/, including all subfolders in /allowed/, but not folders located outside of /allowed/.
- 8** To create folders to organize websites, click the New Folder (folder) button, then double-click the folder to rename it.

To add URLs within a folder, open the folder’s disclosure triangle, select the folder, and then click the Add (+) button.

To create a subfolder, open a folder’s disclosure triangle, select the folder, and then click the New Folder (folder) button.
- 9** To change the name or URL of a website, double-click the website entry; then, to rename a folder, double-click the folder entry.
- 10** To rearrange websites or folders, drag the websites or folders in the list.
- 11** Click Apply Now.

Setting Time Limits and Curfews on Computer Usage

You can use Workgroup Manager to set time limits and curfews for computer usage on computers with Snow Leopard or later.

If you set a time limit for computer usage, users who meet their daily time limits can't log in until the next day when their quota is reset. You can set different time limits for weekdays (Monday through Friday) and weekends (Saturday and Sunday). The time limit can range from 30 minutes to 8 hours.

If you set a curfew, users can't log in during the days and times you specify. If a user is logged in when their curfew starts, the user is immediately logged out. You can set different times for weekdays (denying access Sunday nights through Thursday nights) and weekends (Friday and Saturday nights).

To set time limits and curfews:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Parental Controls and then click Time Limits.
- 5 Set the management setting to Always and then select "Enforce limits."
- 6 To set time limits, click Allowances, then under Weekdays or Weekends select "Limit computer use to" and drag the slider to amount of time you want to limit use.
- 7 To set curfews, click Curfews, select "Sunday through Thursday" or "Friday and Saturday," and then enter the range of time when you want to prevent computer access.
You can highlight the time and replace it with a new time, or you can highlight the time and click the up or down buttons next to the time.
- 8 Click Apply Now.

Managing Printing Preferences

Printer preferences let you control which printers the user can access. Ideally, reduce the printer list to only those printers the user needs to access.

You should require that the user authenticate as an administrator before printing.

To manage Printing preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Printing and then click Printers.
- 5 Set the management setting to Always.
- 6 Click Printer List.
- 7 In the Available Printers list, select a printer and click Add; then add printers that you want the user to access.
- 8 To add additional printers to the user's printer list, click Open Printer Setup.
For more information, see Printer Setup Utility Help.
- 9 Deselect "Allow user to modify the printer list."
- 10 Deselect "Allow printers that connect directly to user's computer."
If you select this setting, select "Require an administrator password."
- 11 Click Access.
- 12 Select a printer, and select "Require an administrator password."
Repeat for all printers in the User's Printer List.
- 13 Click Apply Now.

From the command line:

```
# Managing Printing Preferences
# -----
# Manage printing preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
    RequireAdminToAddPrinters always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
    AllowLocalPrinters always -bool 0
```

Managing Software Update Preferences

With Snow Leopard Server, you can create your own Software Update server to control updates that are applied to specific users or groups. This is helpful because it reduces external network traffic while also providing more control to server administrators.

By configuring a Software Update server, server administrators can choose which updates to provide.

To manage Software Update preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Software Update.
- 5 Set the management setting to Always.
- 6 Specify a URL in the form `http://updateserver.example.com:8088/index.sucatalog`.
- 7 Click Apply Now.

From the command line:

```
# Managing Software Update Preferences
# -----
# Manage Software Update preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.SoftwareUpdate CatalogURL always -string "http:/
$SERVER:8088/index.sucatalog"
```

Managing Access to System Preferences

You can specify which preferences to show in System Preferences. If a user can see a preference, it does not mean the user can modify that preference. Some preferences, such as Startup Disk preferences, require an administrator name and password before a user can modify its settings.

The preferences that appear in Workgroup Manager are those installed on the computer you're using. If your administrator computer is missing preferences that you want to disable on client computers, install the applications related to those preferences or use Workgroup Manager on a computer that includes those preferences.

To manage System Preferences preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click System Preferences.
- 5 Set the management setting to Always.
- 6 Click Show None.
- 7 Select the following items to show in System Preferences:
 - Appearance
 - Select Displays
 - Select Dock
 - Select Expose & Spaces
 - Select Keyboard & Mouse
 - Select Security
 - Select Universal Access
- 8 Click Apply Now.

Managing Universal Access Preferences

Universal Access settings can help improve the user experience. For example, if a user has difficulty using a computer or wants to work in a different way, you can choose settings that enable the user to work more effectively.

Most Universal Access settings do not negatively impact security. However, some settings allow other users to more easily see what you're doing.

To manage Universal Access preferences:

- 1 In Workgroup Manager, click Preferences.
- 2 Make sure the correct directory is selected and you are authenticated.
To switch directories, click the globe icon. If you are not authenticated, click the lock and enter the name and password of a directory domain administrator.
- 3 Select users, groups, computers, or computer groups.
- 4 Click Universal Access.
- 5 Click Seeing and then set the management setting to Always.

6 Deselect Turn on Zoom.

Pressing and holding the Option, Command, and + keys will zoom in, while pressing and holding the Option, Command, and - keys will zoom out.

7 Click Keyboard and select Always.

8 Select Sticky Keys Off and deselect "Show pressed keys on screen."

If Sticky Keys are on and you select "Show pressed keys on screen," modifier keys such as Control, Option, Command, and Shift are displayed on screen. Other keys are not displayed.

9 Click Apply Now.

From the command line:

```
# Managing Universal Access Preferences
#
# -----
# Manage Universal Access preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKey always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKeyBeepOnModifier always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKeyShowWindow always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess closeViewDriver always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess closeViewShowPreview always -bool 0
```

Enforcing Policy

When you implement a policy for controlling the user experience by removing files (from example, Kernel extensions) or by managing user-controllable settings (for example, screen saver settings), you should also implement a mechanism for reenforcing the policy in case the deleted files are restored or the settings are changed by users or by software updates.

Using `mcx`, `cron`, or `launchd` jobs, create scripts that run during startup and shutdown and after software updates to reinforce policy in case of violations.

To protect the policy enforcements scripts, compile them into binary format so users can't modify them.

Use this chapter to learn how to secure NetBoot service.

Securely configuring client configuration management through NetBoot helps standardize the clients across your network and provides a secure deployment.

Network computers can be managed through NetBoot, which decreases maintenance time and can help prevent malicious software attacks.

Securing NetBoot Service

By using NetBoot you can have your client computers start up from a standardized Snow Leopard configuration suited to their specific tasks. Because the client computers start up from the same image, you can quickly update the operating system for an entire group by updating a single boot image.

A *boot image* is a file that looks and acts like a mountable disk or volume. NetBoot images contain the system software needed to act as a startup disk for client computers over the network.

An *installation image* is an image that starts up the client computer long enough to install software from the image. The client can then start up from its own hard drive.

Boot images (NetBoot) and installation images (NetInstall) are different kinds of disk images. The main difference is that a .dmg file is a proper disk image and a .nbi folder is a bootable network volume (which contains a .dmg disk image file). Disk images are files that behave like disk volumes.

For more information about configuring NetBoot service, see the *System Imaging and Software Update Administration* guide.

Disabling NetBoot Service

If your server is not a NetBoot server, disable the NetBoot service. Disabling the service prevents potential vulnerabilities on your computer. The NetBoot service is disabled by default, but verification is recommended.

The best way to prevent clients from using NetBoot on the server is to disable NetBoot service on all Ethernet ports.

To disable NetBoot:

- 1 Open Server Admin and connect to the server.
- 2 Select NetBoot in the Computers & Services list.
- 3 Click General.
- 4 Disable NetBoot on all ports.
- 5 Click Stop NetBoot.

From the command line:

```
# -----
# Securing NetBoot Service
# -----
#
# Disable NetBoot.
#
# -----
sudo serveradmin stop netboot
```

Limit NetBoot Service Clients

If NetBoot service is required, it should be provided over a trusted network.

Securely configure NetBoot service with restrictions on the ports it uses, the images available, and client access to the service. NetBoot service uses Apple Filing Protocol (AFP), Network File System (NFS), Dynamic Host Configuration Protocol (DHCP), Web, and Trivial File Transfer Protocol (TFTP) services, depending on the types of clients your are trying to boot. You must also securely configure services to reduce network vulnerabilities.

NetBoot service creates share points for storing NetBoot and NetInstall images in / Library/NetBoot/ on each volume you enable and names them NetBootSP n , where n is 0 for the first share point and increases by 1 for each extra share point.

For example, if you decide to store images on three server disks, NetBoot service sets up three share points named NetBootSP0, NetBootSP1, and NetBootSP2.

You can restrict access to NetBoot service on a case-by-case basis by listing the hardware addresses (also known as the Ethernet or MAC addresses) of computers that you want to permit or deny access to.

The hardware address of a client computer is added to the NetBoot Filtering list when the client starts up using NetBoot and is, by default, enabled to use NetBoot service. You can specify other services.

To limit NetBoot clients:

- 1 Open Server Admin and connect to the server.
- 2 Select NetBoot in the Computers & Services list.
- 3 Click Settings, then click Filters.

NetBoot service filtering lets you restrict access to the service based on the client's Ethernet hardware (MAC) address. A client's address is added to the filter list the first time it starts up from an image on the server and is allowed access by default.

- 4 Select "Enable NetBoot/DHCP filtering."
- 5 Select "Allow only clients listed below (deny others)" or "Deny only clients listed below (allow others)."
- 6 Use the Add (+) button to enter the canonical or noncanonical form of a hardware address to the filter list, or use the Delete (-) button to remove a MAC address from the filter list.

To look up a MAC address, enter the client's DNS name or IP address in the Host Name field and click Search.

To find the hardware address for a computer using Snow Leopard, look on the TCP/IP pane of the computer's Network preference or run Apple System Profiler.

- 7 Click OK.
- 8 Click Save.

Note: You can also restrict access to a NetBoot image by selecting the name of the image in the Images pane of the NetBoot service settings in Server Admin, clicking the Edit (/) button, and providing the required information.

From the command line:

```
#  
# Securely configure NetBoot.  
# -----  
sudo defaults rename /etc/bootpd allow_disabled allow
```

Viewing NetBoot Service Logs

NetBoot service logging is important to security. With logs, you can monitor and track client communication to the NetBoot server. The NetBoot service log is /var/log/system.log and can be accessed using Server Admin.

To view NetBoot service logs:

- 1 Open Server Admin and connect to the server.
- 2 Select NetBoot in the Computers & Services list.
- 3 Click Logs to display the contents of system.log.

From the command line:

```
#  
# View NetBoot service logs.  
# -----  
sudo tail /var/log/system.log | grep bootpd
```

Use this chapter to learn how to secure Software Update service.

You can protect against attacks by configuring an internal Software Update server. This allows you to maintain a secure network by controlling what software updates are installed on your network computers.

Disabling Software Update Service

If your server is not intended to be a software update server, disable the Software Update service. Disabling the service prevents potential vulnerabilities on your computer. Software Update service is disabled by default, but verification is recommended.

To disable Software Update:

- 1 Open Server Admin and connect to the server.
- 2 Select Software Update in the Computers & Services list.
- 3 Click Settings.
- 4 Click Stop Software Update.
- 5 Click Save.

From the command line:

```
# -----
# Securing Software Update Service
# -----  
  
# Disable Software Update:  
sudo serveradmin stop swupdate
```

Limiting Automatic Update Availability

Software Update service offers you ways to manage Macintosh software updates from Apple on your network. In an uncontrolled environment, users might connect to Apple Software Update servers at any time and update client computers with software that is not approved by your IT group.

By using local Software Update servers, your client computers access only the software updates you permit from software lists that you control, giving you more flexibility in managing computer software updates.

You can restrict client access in a Software Update server by disabling automatic mirror-and-enable functions in the General Settings pane. You manage specific updates in the Updates pane of the Software Update server.

To specify which updates are automatically available as software updates:

- 1** Open Server Admin and connect to the server.
- 2** Select Software Update in the Computers & Services list.
- 3** Click Settings, then click General.
- 4** To immediately disable all software updates for client users, deselect “Automatically enable copied updates.”
- 5** Click Updates.
- 6** In the Enable column, select the checkbox for each update you want to make available to client computers.
- 7** Click Save.

From the command line:

```
#  
# Specify which client can access software updates.  
# -----  
sudo serveradmin settings swupdate:autoEnable = no
```

Viewing Software Update Service Logs

Software Update service logging is important for security. With logs, you can monitor and track communication through the Software Update service. Access the Software Update service log, /var/log/system.log, using Server Admin.

To view Software Update service logs:

- 1 Open Server Admin and connect to the server.
- 2 Select Software Update in the Computers & Services list.
- 3 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
#  
# View Software Update service logs.  
# -----  
sudo tail /var/log/swupd/swupd_*
```

Use this chapter to learn how to use Server Admin and Workgroup Manager to set up and manage home folders, accounts, and settings for clients.

Snow Leopard Server includes Server Admin and Workgroup Manager.

You can use Server Admin to create and manage share points.

You can use Workgroup Manager, a user management tool, to manage user, group, computer, and computer group accounts. You can define core account settings like name, password, home folder location, and group membership. You can also manage preferences, allowing you to customize the user's experience, granting or restricting access to his or her computer's settings and to network resources.

Workgroup Manager works closely with a directory domain. Directory domains are like databases, only they are specifically geared towards storing account information and handling authentication. For more information about Open Directory, see Chapter 23, "Securing Directory Services."

For information about using Workgroup Manager, see the *User Management* guide.

About Open Directory and Active Directory

Snow Leopard Server supports Open Directory and Active Directory domains for client authentication.

Open Directory uses OpenLDAP, the open source implementation of Lightweight Directory Access Protocol (LDAP), to provide directory services. It's compatible with other standards-based LDAP servers, and can be integrated with proprietary services such as Microsoft's Active Directory and Novell's eDirectory. For more information about how to configure these options, see "Configuring Open Directory Policies" on page 329.

The Active Directory plug-in supports packet signing and packet encryption and is set to “allow,” which means it negotiates the connection by default and can be changed to “require” if needed. Also, if you connect to an Active Directory server with Highly Secure (HISEC) templates enabled, you can use third-party tools to further secure your Active Directory connection.

Users can mutually authenticate with Open Directory and Active Directory. Both use Kerberos to authenticate. Kerberos is a ticket-based system that enables mutual authentication.

The server must identify itself by providing a ticket to a users’ computer. This prevents your computer from connecting to rogue servers. Users must enable trusted binding to mutually authenticate with Open Directory or Active Directory.

For more information about Open Directory and Active Directory, see the *Open Directory Administration* guide.

Securing Directory Accounts

You can modify several account settings to improve security. Check with your organization to ensure that these settings do not conflict with network settings or organizational requirements.

In Workgroup Manager, you can use presets to save your settings as a template for future accounts. If you have settings that apply to several accounts, use presets to expedite the creation of these accounts. Using presets also ensures that you use uniform account settings and helps you avoid configuration errors. For more information, see the *User Management* guide.

Configuring Directory User Accounts

If you want to manage individual users or if you want those users to have unique identities on your network, create user accounts.

Before creating or modifying user accounts, you should have a firm understanding of what the account will be used for and what authentication method you want to use.

To configure user accounts:

- 1 In Workgroup Manager, click Accounts.
- 2 Select the directory domain where the account resides by clicking the small globe icon, and then authenticate as the domain administrator.

To authenticate, click the lock and enter the name and password of a directory domain administrator.

- 3 Select the user account you want to work with from the user accounts list.
- 4 Click Basic.

- 5 If you want to grant server administration privileges to the user, select “administer this server.”

Server administration privileges allows the user to use Server Admin and make changes to a server’s search policy using Directory Utility.

- 6 Click Advanced, then deselect “Allow simultaneous login on managed computers.”

By disallowing simultaneous login, you reduce the chances of version conflicts when loading and saving files. This helps remind users that they should log off of computers when they are not using them.

- 7 Choose the most secure password type available in the User Password Type pop-up menu.

If you don’t use smart cards, you can choose Open Directory or crypt password. Open Directory is more secure than crypt password. If your network uses Open Directory for authentication, authenticate with it. For more information about Open Directory and crypt passwords, see the *Open Directory Administration* guide.

Smart cards are also a secure form of authentication. Smart cards use two-factor authentication, which helps ensure that your accounts are not compromised.

- 8 If you chose the Open Directory password type, click Options and complete the following:

- a In the dialog that appears, select “Disable login on specific date” and enter the date that the user no longer needs the account.
- b Select “Disable login after inactive for # days,” and replace # with the number of days when the user no longer needs the account.
- c Select “Disable login after user makes # failed attempts,” and replace # with 3.
- d Select “Allow the user to change the password.”
- e Select “Password must contain at least # characters,” and replace # with 8.
- f Select “Password must be reset every # days,” and replace # with 90.
- g If you want to require the user to create a password during their next login, select “Password must be changed at next login.”
- h Replace these suggested values with values that meet the requirements of your organization.
- i Click OK.

- 9 Click Groups.

- 10 Click the Add (+) button to open a drawer listing all available groups, then drag groups from the drawer into the Primary Group ID field or the Other Groups list.

A primary group is the group a user belongs to if the user does not belong to other groups. If a user selects a different workgroup at login, the user still retains access permissions from the primary group.

The ID of the primary group is used by the file system when the user accesses a file he or she doesn't own. The file system checks the file's group permissions, and if the primary group ID of the user matches the ID of the group associated with the file, the user inherits group access permissions.

Adding a user to a group allows the user to access the group's group folder. Carefully choose which groups to add users to. For more information, see "Configuring Group Accounts" on page 321.

- 11 Click Home.
- 12 Select a secure location for the user's home folder in the home list and then enter an appropriate value in the Disk Quota field.

By using a disk quota, you prevent malicious users from performing a denial of service attack where they fill the home volume.
- 13 Click Mail and select None.

If you must enable mail, select POP only or IMAP only, but not both. Using fewer protocols reduces the number of possible avenues of attack.
- 14 Click Info.
- 15 Do not enter information in the user information fields provided.

User information can be used by malicious attackers when they try to compromise the user's account.
- 16 Click Windows and then click Save.

Configuring Group Accounts

Create groups of individuals with similar access needs. For example, if you create a separate group for each office, you can specify that only members of a certain office can log in to specific computers. When you more specifically define groups, you have greater control over who can use what.

You can grant or deny POSIX or ACL permissions to groups. If you have nested groups, you can propagate ACL permissions to child groups.

Groups also have access to group folders, which provide an easy way for group members to share files with each other.

To configure group accounts:

- 1 In Workgroup Manager, click Accounts.
- 2 Select the directory domain where the group account resides by clicking the small globe icon, and then authenticate as the domain administrator.

To authenticate, click the lock and enter the name and password of a directory domain administrator.
- 3 Select the group account you want to work with from the group accounts list.

- 4** In the Members pane, click the Add (+) button to open a drawer that lists the users and groups defined in the directory domain you're working with.

Make sure the group account resides in a directory domain specified in the search policy of computers that the user logs in to.

- 5** Click Group Folder.
- 6** In the Address list select a secure location for the group folder.
- 7** In the Owner Name fields, enter the short name and long name of the user you want to assign as the owner of the group folder so the user can act as group folder administrator.

To choose an owner from a list of users in the current directory domain, click the browse (...) button. Click the globe icon in the drawer to choose a different directory domain.

The group folder owner is given read/write access to the group folder.

- 8** Click Save.

Configuring Computer Groups

A computer group comprises computers with the same preference settings. You can use Workgroup Manager to create and modify computer groups.

Every computer on your network should be a member of a computer group. If you don't assign a computer to a computer group, the computer uses the managed preferences for the Guest Computer account.

By grouping computers into computer groups, you simplify the task of securing computers on your network.

To configure computer groups:

- 1** In Workgroup Manager, click Accounts.
- 2** Select the directory domain where the computer group resides by clicking the small globe icon, and then authenticate as the domain administrator.
To authenticate, click the lock and enter the name and password of a directory domain administrator.
- 3** Select the compute group you want to work with from the user accounts list.
- 4** Click Members, click the Add (+) button, and then drag computers or computer groups from the drawer to the list.

You can also click the browse (...) button, select a computer, and then click Add.

Continue adding computers and computer groups until the list is complete.

- 5** Click Save.

Controlling Network Views

Snow Leopard Server doesn't support managed network views.

To manage network views hosted on servers running Tiger Server, use the Workgroup Manager included with Tiger Server.

Use this chapter to learn how to secure Directory service.

Directory services are the backbone of your network's security policy. The granting of access to the information and services on your network should be well-planned and thought out.

A directory service provides a central repository for information about computer users and network resources in an organization. Snow Leopard Server uses Open Directory for its directory service.

The directory services provided by Snow Leopard Server use LDAPv3, as do many other servers. LDAPv3 is an open standard common in mixed networks of Macintosh, UNIX, and Windows systems. Some servers use the older version, LDAPv2, to provide directory service.

Open Directory also provides authentication service. It can securely store and validate the passwords of users who want to log in to client computers on your network or use other network resources that require authentication. Open Directory can also enforce policies such as password expiration and minimum length.

For more information about passwords and authentication, see Appendix A, "Understanding Passwords and Authentication," on page 380.

Open Directory must be set to the proper role and configured to use SSL to encrypt its communications to protect the confidentiality of its important authentication data. Password policies can also be enforced by Open Directory.

For more information about understanding and configuring directory and authentication services, see the *Open Directory Administration* guide.

Open Directory Server Roles

Open Directory can be configured to one of several roles, depending on the server's place in the network and directory structure:

- Standalone Server—This role does not share information with other computers on the network. It is a local directory domain only.
- Connected to a Directory Server—This role allows the server to get directory and authentication information from another server's shared directory domain.
- Open Directory Master—This role provides an Open Directory Password Server, which supports conventional authentication methods required by Snow Leopard Server services. In addition, an Open Directory Master can provide Kerberos authentication for single sign-on.
- Open Directory Replica—This role acts as a backup to the Open Directory master. It can provide the same directory and authentication information to other networks as the master. It has a read-only copy of the master's LDAP directory domain.

Configuring the Open Directory Services Role

If the server is not a directory server, make sure the LDAP server is stopped using Server Admin. To stop LDAP server, set the Open Directory role to Standalone Server. This prevents Open Directory from engaging in unnecessary network communications.

On a newly installed server, the LDAP server should be stopped by default, but verification is recommended.

To configure the Open Directory role:

- 1 Open Server Admin and connect to the server.
- 2 Select Open Directory in the Computers & Services list.
- 3 Click Settings, then click General.
- 4 Click Change.

The Service Configuration Assistant opens.

- 5 Choose a role, then click Continue.
- 6 Confirm the Open Directory configuration settings, then click Continue.
- 7 If the server was an Open Directory master and you are sure that users and services no longer need access to the directory data stored in the shared directory domain that the server has been hosting, click Close.

- 8 Click the Open Directory Utility button to configure access to directory systems.
- 9 If the server you're configuring has access to a directory system that also hosts a Kerberos realm, you can join the server to the Kerberos realm.

To join the Kerberos realm, you need the name and password of a Kerberos administrator or a user who has the authority to join the realm.
- 10 Click Save.

From the command line:

```
# -----
# Securing Directory Services
# -----
# Configure the Open Directory role:
sudo slapconfig -createldapmasterandadmin $ADMIN $ADMIN_FULL_NAME
$ADMIN_UID $SEARCH_BASE $REALM
```

Starting Kerberos After Setting Up an Open Directory Master

If Kerberos doesn't start when you set up an Open Directory master, you can use Server Admin to start it manually, but first you must fix the problem that prevented Kerberos from starting. Usually the problem is that the DNS service isn't correctly configured or isn't running.

Note: After you manually start Kerberos, users whose accounts have Open Directory passwords and were created in the Open Directory master's LDAP directory while Kerberos was stopped might need to reset their passwords the next time they log in. A user account is therefore affected only if all recoverable authentication methods for Open Directory passwords were disabled while Kerberos was stopped.

To start Kerberos manually on an Open Directory master:

- 1 Open Server Admin and connect to the server.
- 2 Select Open Directory in the Computers & Services list.
- 3 Click Refresh (or choose View > Refresh) and verify the status of Kerberos as reported in the Overview pane.

If Kerberos is running, there's nothing more to do.

- 4 Verify that the DNS name and address resolve by using Network Utility (in / Applications/Utilities/) to do a DNS lookup of the Open Directory master's DNS name and a reverse lookup of the IP address.

If the server's DNS name or IP address doesn't resolve correctly:

- In the Network pane of System Preferences, look at the TCP/IP settings for the server's primary network interface (usually built-in Ethernet). Make sure the first DNS server listed is the one that resolves the Open Directory server's name.
 - Check the configuration of DNS service and make sure it's running.
- 5 In Server Admin, select Open Directory for the master server, click Settings, then click General.
- 6 Click Kerberize, then enter the following information:
- *Administrator Name and Password*: You must authenticate as an administrator of the Open Directory master's LDAP directory.
 - *Realm Name*: This field is preset to be the same as the server's DNS name converted to capital letters. This is the convention for naming a Kerberos realm. If necessary, you can enter a different name.

From the command line:

```
# Start Kerberos manually on an Open Directory master:  
sudo kdcsetup -a $ADMIN $REALM
```

Configuring Open Directory for SSL

Using Server Admin, you can enable Secure Sockets Layer (SSL) for encrypted communications between an Open Directory server's LDAP directory domain and computers that access it.

SSL uses a digital certificate to provide a certified identity for the server. You can use a self-signed certificate or a certificate obtained from a CA.

SSL communications for LDAP use port 636. If SSL is disabled for LDAP service, communications are sent as clear text on port 389.

To set up SSL communications for LDAP service:

- 1 Open Server Admin and connect to the Open Directory master or an Open Directory replica server.
- 2 Select Open Directory in the Computers & Services list.
- 3 Click Settings, then click LDAP.
- 4 From the Configure pop-up menu, choose LDAP Settings, then select Enable SSL.
- 5 Use the Certificate pop-up menu to choose an SSL certificate that you want LDAP service to use.

The menu lists all SSL certificates installed on the server. To use a certificate not listed, choose Custom Configuration from the pop-up menu.

- 6 Click Save.

From the command line:

The following steps describe the command-line method for creating certificates. For information about defining, obtaining, and installing certificates on your server using Certificate Manager in Server Admin, see “Readyng Certificates” on page 168.

To create an Open Directory service certificate:

- 1 Generate a private key for the server in the /usr/share/certs/ folder:

If the /usr/share/certs folder does not exist create it.

```
sudo openssl genrsa -out ldapserver.key 2048
```

- 2 Generate a CSR for the CA to sign:

```
sudo openssl req -new -key ldapserver.key -out ldapserver.csr
```

- 3 Fill out the following fields as completely as possible, making certain that the Common Name field matches the domain name of the LDAP server exactly:

Country Name:

Organizational Unit:

State or Province Name:

Common Name:

Locality Name (city):

Email Address:

Organization Name:

Leave the challenge password and optional company name blank.

- 4 Sign the ldapserver.csr request with the openssl command.

```
sudo openssl ca -in ldapserver.csr -out ldapserver.crt
```

- 5 When prompted, enter the CA passphrase to continue and complete the process.

The certificate files needed to enable SSL on the LDAP server are now in the /usr/share/certs/ folder.

- 6 Open Server Admin.

- 7 In the Computers & Services list, select Open Directory for the server that is an Open Directory master or an Open Directory replica.

- 8 Click Settings.

- 9 Click Protocols.

- 10 From the Configure pop-up menu, choose “LDAP Settings.”

- 11 Select Enable Secure Sockets Layer (SSL).

- 12 Use the Certificate pop-up menu to choose an SSL certificate that you want LDAP service to use.

The menu lists SSL certificates that have been installed on the server. To use a certificate not listed, choose Custom Configuration from the pop-up menu.
- 13 Click Save.

Configuring Open Directory Policies

You can set password, binding, and security policies for an Open Directory master and its replicas. You can also set several LDAP options for an Open Directory master or replica.

For more information about configuring policies, see “Configuring Directory User Accounts” on page 319.

Setting the Global Password Policy

Using Server Admin, you can set a global password policy for user accounts in a Snow Leopard Server directory domain.

The global password policy affects user accounts in the server’s local directory domain. If the server is an Open Directory master or replica, the global password policy also affects user accounts that have an Open Directory password type in the server’s LDAP directory domain.

If you change the global password policy on an Open Directory replica, the policy settings become synchronized with the master and replicas.

Administrator accounts are exempt from password policies. Each user can have a password policy that overrides global password policy settings. For more information, see “Password Policies” on page 387.

Kerberos and Open Directory Password Server maintain password policies separately. Snow Leopard Server synchronizes the Kerberos password policy rules with Open Directory Password Server password policy rules.

To change the global password policy of user accounts in the same domain:

- 1 Open Server Admin and connect to an Open Directory master or replica server.
- 2 Select Open Directory in the Computers & Services list.
- 3 Click Settings, then click Policy.
- 4 Click Passwords.

This allows you to set password policy options you want enforced for users who do not have individual password policies.

5 Select the following:

- "After user makes 3 failed attempts."
- "Differ from account name."
- "Contain at least one letter."
- "Contain at least one numeric character."
- "Be reset on first user login."
- "Contain at least 12 characters."
- "Differ from last 3 passwords used."
- "Be reset every 3 months."

Note: If you select an option that requires resetting the password, remember that some service protocols don't permit users to change passwords. For example, users can't change their passwords when authenticating for IMAP mail service.

6 Click Save.

Replicas of the Open Directory master automatically inherit its global password policy.

From the command line:

```
#  
# Change the global password policy of user accounts in the same domain.  
# -----  
sudo pwpolicy -a $ADMIN_USER -setglobalpolicy "usingHistory=3 requiresAlpha  
requiresNumeric maxMinutesUntilChangePassword=131487 minChars=12  
maxFailedLoginAttempts=3"
```

Setting a Binding Policy for an Open Directory Master and Replicas

Using Server Admin, you can configure an Open Directory master to permit or require trusted binding between the LDAP directory and the computers that access it. Replicas of an Open Directory master inherit the master's binding policy.

Trusted LDAP binding is mutually authenticated. The computer proves its identity by using an LDAP directory administrator's name and password to authenticate to the LDAP directory. The LDAP directory proves its authenticity by means of an authenticated computer record created in the directory when you set up trusted binding.

Clients can't be configured to use trusted LDAP binding and a DHCP-supplied LDAP server (also known as DHCP option 95). Trusted LDAP binding is inherently a static binding, but DHCP-supplied LDAP is a dynamic binding.

Note: To use trusted LDAP binding, clients need Tiger or Tiger Server or later. Clients using Mac OS X v10.3 or earlier can't set up trusted binding.

To set the binding policy for an Open Directory master:

- 1 Open Server Admin and connect to the Open Directory master server.
- 2 Click the triangle at the left of the server.
The list of services appears.
- 3 From the expanded Servers list, select Open Directory.
- 4 Click Settings, then click Policy.
- 5 Click Binding, then set the directory binding options you want:
 - To *permit* trusted binding, select “Enable authenticated directory binding.”
 - To *require* trusted binding, also select “Require authenticated binding between directory and clients.”
- 6 Click Save.

Important: If you enable “Encrypt all packets (requires SSL or Kerberos)” and “Enable authenticated directory binding,” make sure users use only one for binding and not both.

From the command line:

```
#  
# Set the binding policy for an Open Directory master.  
# -----  
sudo slapconfig -setmacosxodpolicy -binding required
```

Setting a Security Policy for an Open Directory Master and Replicas

Using Server Admin, you can configure a security policy for access to the LDAP directory of an Open Directory master.

Replicas of the Open Directory master inherit the master’s security policy.

Note: If you change the security policy for the LDAP directory of an Open Directory master, you must disconnect and reconnect (unbind and rebind) every computer connected (bound) to this LDAP directory using Directory Utility.

To set the security policy for an Open Directory master:

- 1 Open Server Admin and connect to the Open Directory master server.
- 2 Select Open Directory in the Computers & Services list.
- 3 Click Settings, then click Policy.

4 Click Binding, then set the security options you want:

- “**Disable clear text passwords**” determines whether clients can send passwords as clear text if the passwords can’t be validated using any authentication method that sends an encrypted password.
- “**Digitally sign all packets (requires Kerberos)**” certifies that directory data from the LDAP server won’t be intercepted and modified by another computer while en route to client computers.
- “**Encrypt all packets (requires SSL or Kerberos)**” requires the LDAP server to encrypt directory data using SSL or Kerberos before sending it to client computers.
- “**Block man-in-the-middle attacks (requires Kerberos)**” protects against a rogue server posing as the LDAP server. Best if used with the “Digitally sign all packets” option.
- “**Disable client-side caching**” prevents client computers from caching LDAP data locally.
- “**Allow users to edit their own contact information**” permits users to change contact information on the LDAP server.

5 Click Save.

From the command line:

```
#  
# Set the security policy for an Open Directory master.  
# -----  
sudo slapconfig -setmacosxodpolicy -cleartext blocked -encrypt yes  
-sign yes -man-in-the-middle blocked -clientcaching no
```

Use this chapter to learn how to secure RADIUS.

By configuring a RADIUS (Remote Authentication Dial In User Service) server with Open Directory, you can secure your wireless environment from unauthorized users.

Wireless networking gives companies greater network flexibility, seamlessly connecting laptop users to the network and giving them the freedom to move within the company while staying connected to the network.

This chapter describes how to configure and use RADIUS to keep your wireless network secure and to make sure it is used only by authorized users.

Disabling RADIUS

If your server is not intended to be a RADIUS server, disable RADIUS. Disabling the service prevents potential vulnerabilities on your computer. RADIUS is disabled by default, but verification is recommended.

To disable RADIUS:

- 1 Open Server Admin and connect to the server.
- 2 Select RADIUS in the Computers & Services list.
- 3 Click Stop RADIUS.
- 4 Click Save.

From the command line:

```
# -----  
# Securing RADIUS Service  
# -----  
  
# Disable RADIUS  
sudo serveradmin stop radiusc
```

Securely Configuring RADIUS Service

RADIUS is used to authorize Open Directory users and groups so they can access Airport Base Stations on a network. By configuring RADIUS and Open Directory you can control who has access to your wireless network.

RADIUS works with Open Directory and Password Server to grant authorized users access to the network through an Airport Base Station. When a user attempts to access an Airport Base Station, Airport communicates with the RADIUS server using Extensible Authentication Protocol (EAP) to authenticate and authorize the user.

Users are given access to the network if their user credentials are valid and they are authorized to use the Airport Base Station. If a user is not authorized, he or she cannot access the network through the Airport Base Station.

Configuring RADIUS to Use Certificates

To increase the security and manageability of Airport Base Stations, use Server Admin to configure RADIUS to use custom certificates. Using a certificate increases the security and manageability of Airport Base Stations.

To use a custom certificate:

- 1 Open Server Admin and connect to the server.
- 2 Select RADIUS in the Computers & Services list.
- 3 Click Settings.
- 4 From the RADIUS Certificate pop-up menu, choose a certificate.

If you have a custom certificate, choose Custom Configuration from the Certificate pop-up menu and enter the path to the certificate file, private key file, and certificate authority file. If the private key is encrypted, enter the private key passphrase and click OK.

If you don't have a certificate and want to create one, click Manage Certificates. For more information about creating certificates, see Chapter 9, "Managing Certificates."

- 5 Click Save.

From the command line:

```
# Use a custom certificate:  
sudo serveradmin settings radius:eap.conf:CA_file = "/etc/certificates/  
$CA_CRT"  
sudo serveradmin settings radius:eap.conf:private_key_file = "/etc/  
certificates/$KEY"  
sudo serveradmin settings radius:eap.conf:private_key_password = "$PASS"  
sudo serveradmin settings radius:eap.conf:certificate_file = "/etc/  
certificates/$CERT"
```

Editing RADIUS Access

You can restrict access to RADIUS by creating a group of users and adding them to the service access control list (SACL) of RADIUS.

To edit RADIUS access:

- 1 Open Server Admin and connect to the server.
- 2 Select RADIUS in the Computers & Services list.
- 3 Click Settings, then click Edit Allowed Users.
- 4 Select “For selected services below,” then select RADIUS.
- 5 Select “Allow only users and groups below.”
- 6 Click the Add (+) button.
- 7 From the Users and Groups list, drag users or groups of users to the “Allow only users and groups below” list.

If you want to remove users from the “Allow only users and groups below” list, select the users or groups of users and click the Delete (-) button. The user’s in this list are the only ones who can use RADIUS.

From the command line:

```
#  
# Edit RADIUS access.  
# -----  
sudo dseditgroup -o edit -a $USER -t user com.apple.access_radius
```

Viewing RADIUS Service Logs

RADIUS logging is important for security. With logs, you can monitor and track communication through RADIUS . You can access the RADIUS log, /var/log/system.log, using Server Admin.

To view the RADIUS log:

- 1 Open Server Admin and connect to the server.
- 2 Select RADIUS in the Computers & Services list.
- 3 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
#  
# View the RADIUS log  
# -----  
sudo tail /var/log/radius/radius.log
```

Use this chapter to learn how to secure print service.

Print service is often an overlooked part of a security configuration. Important information passes into your networked printers so it is important that your printers are not misused.

With a print server, you can share printers by setting up print queues accessible by any number of users over a network connection. When a user prints to a shared queue, the print job waits on the server until the printer is available or until established scheduling criteria are met.

Apple's printing infrastructure is built on Common UNIX Printing System (CUPS). CUPS uses open standards such as Internet Printing Protocol (IPP) and PostScript Printer Description files (PPDs).

For more information about configuring print service, see the *Print Server Administration* guide.

Disabling Print Service

If your server is not intended to be a print server, disable the print server software. Disabling the service prevents potential vulnerabilities on your computer. Print service is disabled by default, but verification is recommended.

To disable print service:

- 1 Open Server Admin and connect to the server.
- 2 Select Print in the Computers & Services list.
- 3 Click Stop Print.

From the command line:

```
# -----  
# Securing Print Service  
# -----  
#  
# Disable print service.  
# -----  
sudo serveradmin stop print
```

Securing Print Service

To increase security of your print service, configure service access controls and Kerberos.

Configuring Print Service Access Control Lists (SACLs)

You can configure SACLs using Server Admin. SACLs enable you to specify which administrators have access to print service.

SACLs provide you with greater control over which administrators have access to monitor and manage a service. The users and groups listed in a service's SACL are the only ones who can access the service. For example, to give administrator access to users or groups for the print service on your server, add them to the print service SACL.

To set administrator SACL permissions for print service:

- 1 Open Server Admin and connect to the server.
- 2 Select the server's name.
- 3 Click Access.
- 4 Click Administrators.
- 5 Select the level of restriction that you want for the services.

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

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

- 6 To open the Users and Groups list, click the Add (+) button.
- 7 Drag users and groups from Users and Groups to the list.
- 8 Set the user's permission.

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

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

- 9 Click Save.

From the command line:

```
# Set administrator SACL permissions for print service:  
sudo dseditgroup -o edit -a $USER -t user com.apple.monitor_print
```

Configuring Kerberos

You can configure Kerberos support for print service IPP shared queues using CUPS v1.3 online web tools. The print service then uses the local Kerberos server to authorize clients to print.

For your client computers to use Kerberos with print service, the clients must be part of the same Kerberos realm. For information on how to join your client computers to a Kerberos realm, see *Open Directory Administration*.

In addition to joining the Kerberos realm, client computers must also use CUPS online web tools to configure Kerberos settings. The steps for configuring CUPS are the same on the client and server computers.

To configure Kerberos for print service:

- 1 Open Safari browser.
- 2 Navigate to the CUPS online web administration tool at <http://localhost:631>.
- 3 Click the Administration tab.
- 4 Under Basic Server Settings, select the “Use Kerberos Authentication” checkbox.
- 5 Click Change Settings and authenticate if prompted.

Print service is restarted and Kerberos is enabled.

You can also edit the configuration file in CUPS by clicking Edit Configuration File in the Administration tab to open the /etc/cups/cupsd.conf file. Change the default authentication type from Basic to Negotiate, as shown:

```
# Default authentication type, when authentication is required...  
DefaultAuthType Negotiate
```

From the command line:

```
#  
# Configure Kerberos for print service.  
# -----  
sudo serveradmin settings sudo serveradmin settings print:authType =  
    KERBEROS
```

Configuring Print Queues

If print service is required, create a print queue for shared printers that is accessible by users over a network connection.

AppleTalk and Line Printer Remote (LPR) printer queues do not support authentication. Print service relies on the client to provide user information. Although standard Macintosh and Windows clients provide correct information, a clever user could potentially modify the client to submit false information and avoid print quotas.

SMB service supports authentication, requiring users to log in before using SMB printers. Print service uses Basic and Digest (MD5) authentication and supports the IPP print job submission method.

You can share any printer that is set up in a print queue on the server. You create print queues using Server Admin.

To create a print queue:

- 1 Open Server Admin and connect to the server.
- 2 Select Print in the Computers & Services list.
- 3 Click Queues.
- 4 Click the Add (+) button to add a print queue for a specific printer, and provide the following printer information for the printer the queue is created for:

From the pop-up menu, choose the protocol used by the printer.

For an LPR printer, enter the printer IP address or DNS name and click OK.

For an Open Directory printer, select the printer in the list and click OK.

- 5 Enter the Internet address or DNS name for the printer.

If you don't want to use the printer's default queue, deselect "Use default queue on server," enter a queue name, and click OK.

- 6 Select the queue you added to the queue list.

To verify that you selected the correct queue, make sure the queue name matches the name next to Printer.

Note: Changing the Sharing Name also changes the queue name that appears in Print & Fax preferences on the server.

- 7 In the Sharing Name field, enter the queue name you want clients to see.

Make sure the name is compatible with naming restrictions imposed by your clients. For example, some LPR clients do not support names that contain spaces, and some Windows clients restrict names to 12 characters. Queue names shared using LPR or SMB must not contain characters other than A–Z, a–z, 0–9, and _ (underscore).

AppleTalk queue names cannot be longer than 32 bytes. This might be fewer than 32 typed characters. The queue name is encoded according to the language used on the server and might not be readable on client computers using another language.

- 8 Select the printing protocols your clients use.

If you select "SMB," make sure you start SMB service.

- 9 If you want to enforce the print quotas you establish for users in Workgroup Manager, select the "Enforce quotas for this queue" checkbox.

- 10 If you want the printer to create a cover sheet, choose the title of the cover sheet from the Cover Sheet pop-up menu; otherwise, choose "None."

- 11 Click Save.

From the command line:

```
#  
# Configure a Print queue.  
# -----  
sudo serveradmin settings print:lprQueues:_array_index:0 =  
    $PRINTER_SHARING_NAME  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:sharingName =  
    $PRINTER_SHARING_NAME  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:quotasEnforced = yes  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:showNameInBonjour = no  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:defaultCoverPage =  
    "classified"  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:sharingList:_array_index:0:ser  
    vice = "IPP"  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:sharingList:_array_index:0:sha  
    ringEnable = yes  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:printerURI = "lpd://  
    example.com"  
sudo serveradmin settings print:queuesArray:_array_id:example_com:shareable  
    = yes  
sudo serveradmin settings  
    print:queuesArray:_array_id:example_com:printerName = "example_com"  
sudo serveradmin settings print:useRemoteQueues = yes  
sudo serveradmin settings print:coverPageNames:_array_index:0 =  
    "classified"
```

Viewing Print Service and Queue Logs

Print service keeps two types of logs: a print service log and individual print queue logs.

- The print service log records the time of events such as when print service is started and stopped and when a print queue is put on hold.
- A print queue log records information such as the name of users who submitted jobs and the size of each job.

You can view print service logs using Server Admin.

To view print service logs:

- 1 Open Server Admin and connect to the server.
- 2 Select Print in the Computers & Services list.
- 3 Click Logs.

Use the Filter field to search for specific entries.

From the command line:

```
#  
# View print service logs.  
# -----  
sudo tail /Library/Logs/PrintService/PrintService_admin.log
```

Use this chapter to learn how to secure Multimedia services.

Protecting QuickTime multimedia streams and only allowing access to those who are authorized to view them can help keep information private. The following section helps you understand and configure QuickTime Streaming Server (QTSS) securely.

Streaming is the delivery of media, such as movies and live presentations, over a network in real time. A computer (streaming server) sends the media to another computer (client computer), which plays the media as it is delivered.

With QTSS software, you can deliver:

- Broadcasts of live events in real time
- Video on demand
- Playlists of prerecorded content

A level of security is inherent in real-time streaming, because content is delivered only as the client needs it and no files remain afterward, but you might need to address some security issues.

For more information about configuring multimedia services, see the *QuickTime Streaming and Broadcasting Administration* guide.

Disabling QTSS

If your server is not intended to be a QuickTime streaming server, disable the QuickTime Streaming server software. Disabling the software prevents potential vulnerabilities on your computer. QTSS is disabled by default, but verification is recommended.

To disable QTSS:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Stop QuickTime Streaming.

From the command line:

```
# -----
# Securing Multimedia Services
# -----
#
# Disable QTSS.
# -----
sudo serveradmin stop qtss
```

Securely Configuring QTSS

A level of security is inherent in real-time streaming because content is delivered only as the client needs it and no files remain afterward. However, you might need to address some security issues.

The streaming server uses the IETF standard RTSP/RTP protocols. RTSP runs on top of TCP and RTP runs on UDP. Many firewalls are configured to restrict TCP packets by port number, and are very restrictive on UDP.

There are three options for streaming through firewalls with QTSS. These options are not mutually exclusive. Typically one or more are used to provide the most flexible setup. The three configurations outlined below are for clients behind a firewall.

- **Stream via port 80:** This option enables the streaming server to encapsulate RTSP and RTP traffic inside TCP port 80 packets. Because this is the default port used for HTTP-based web traffic, the streamed content gets through most firewalls. However, encapsulating the streaming traffic lowers performance on the network and requires faster client connections to maintain streams. It also increases load on the server.
- **Open the appropriate ports on the firewall:** This option allows the streaming server to be accessed via RTSP/RTP on the default ports, and provides better use of network resources, lower speeds for client connections, and less load on the server. The ports that must be open include:
 - TCP port 80: Used for signaling and streaming RTSP/HTTP (if enabled on server).
 - TCP port 554: Used for RTSP.
 - UDP ports 6970–9999: Used for UDP streaming. A smaller range of UDP ports, typically 6970–6999, can usually be used.
 - TCP port 7070: Optionally used for RTSP. (Real Server uses this port; QTSS/Darwin can also be configured to use this port.)
 - TCP ports 8000 and 8001: Can be opened for Icecast MP3 streaming.

- **Set up a streaming proxy server:** The proxy server is placed in the network demilitarized zone (DMZ)—an area on the network that is between an external firewall that connects to the Internet and an internal firewall between the DMZ and the internal network.

Using firewall rules, packets with the ports defined above are allowed from the proxy server to clients through the internal firewall, and also between the proxy server and the Internet via the external firewall. However, clients are not allowed to make direct connections to external resources over those ports.

This approach ensures that all packets bound for the internal network come through the proxy server, providing an additional layer of network security.

Configuring a Streaming Server

If you require QTSS, configure it in conjunction with your firewall and bind it to a single IP address.

To configure a streaming server:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Settings.
- 3 Click IP Binding.

By binding QTSS with an IP address, you can easily track network activity. You can also configure the firewall to restrict network access to this IP address. IP binding is also helpful when your server is multihomed (for example, if you’re also hosting a web server).

- 4 Select the IP address from the list.
- 5 Click Save.
- 6 Click Start QuickTime Streaming.

From the command line:

```
#  
# Configure a streaming server.  
# -----  
sudo serveradmin settings qtss:server:bind_ip_addr:_array_index:0 =  
    "$BIND_IP_ADDRESS"
```

Serving Streams Through Firewalls Using Port 80

If you are setting up a streaming server on the Internet and some of your clients are behind firewalls that allow only web traffic, enable streaming on port 80.

With this option, the streaming server accepts connections on port 80, the default port for web traffic, and QuickTime clients can connect to your streaming server even if they are behind a web-only firewall.

If you enable streaming on port 80, make sure you disable any web server with the same IP address to avoid conflicts with your streaming server.

To serve QuickTime streams over HTTP port 80:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Settings.
- 3 Click IP Bindings.
- 4 Select “Enable streaming on port 80.”

Streaming for selected addresses must be enabled.

Important: If you enable streaming on port 80, make sure your server is not also running a web server, such as Apache. Running QTSS and a web server with streaming on port 80 enabled can cause a port conflict that results in one or both servers not behaving properly.

From the command line:

```
# Serve QuickTime streams over HTTP port 80:  
sudo serveradmin settings qtss:server:rtsp_port:_array_index:0 =  
    554qtss:server:rtsp_port:_array_index:1 =  
    80qtss:server:rtsp_port:_array_index:2 =  
    8000qtss:server:rtsp_port:_array_index:3 = 8001
```

Streaming Through Firewalls or Networks with Address Translation

The streaming server sends data using UDP packets. Firewalls designed to protect information on a network often block UDP packets. As a result, client computers located behind a firewall that blocks UDP packets can't receive streamed media.

However, the streaming server also allows streaming over HTTP connections, which allows streamed media to be viewed through even very tightly configured firewalls.

Some client computers on networks that use address translation cannot receive UDP packets, but they can receive media that's streamed over HTTP connections.

If users have problems viewing media through a firewall or via a network that uses address translation, have them upgrade their client software to QuickTime 5 or later. If users still have problems, have their network administrators provide them with the relevant settings for the streaming proxy and streaming transport settings on their computers.

Network administrators can also set firewall software to permit RTP and RTSP throughput.

Changing the Password Required to Send an MP3 Broadcast Stream

Broadcasting MP3s to another server requires authentication.

To change the MP3 broadcast password:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Settings, then click Access.
- 3 In the MP3 Broadcast Password box, enter a new password.
- 4 Click Save.

From the command line:

```
# Change the MP3 broadcast password:  
sudo serveradmin settings  
qtss:modules:_array_id:QTSSMP3StreamingModule:mp3_broadcast_password =  
    "$QTMP3_PASSWORD"
```

Using Automatic Unicast (Announce) with QTSS on a Separate Computer

You can broadcast from QuickTime Broadcaster to QTSS. This setting can also be used to receive Announced UDP streams from another QuickTime streaming server via a relay using the Automatic Unicast (Announce) transmission method. To do so, you must create a broadcast user name and password on the streaming server.

To create a broadcast user name and password on the streaming server:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Settings, then click Access.
- 3 Click the “Accept incoming broadcasts” checkbox.
- 4 Click Set Password and enter the name and password.
- 5 Click Save.

From the command line:

```
#  
# Create a broadcast user name and password on the streaming server.  
# -----  
sudo serveradmin settings  
qtss:modules:_array_id:QTSSReflectorModule:allow_broadcasts = yes
```

Controlling Access to Streamed Media

You can set up authentication to control client access to streamed media files. You can use Workgroup Manager to specify who can access the media files, or you can use an access file.

Two schemes of authentication are supported: basic and digest. By default, the server uses the more secure digest authentication.

You can also control playlist access and administrator access to your streaming server. Authentication does not control access to media streamed from a relay server. The administrator of the relay server must set up authentication for relayed media.

The ability to manage user access is built into QTSS, so it is always enabled.

For access control to work, an access file must be present in the directory you selected as your media directory. If an access file is not present in the QTSS media directory, all clients are allowed access to the media in the directory.

To control access using Open Directory:

- Authorize each user in Workgroup Manager.

For more information, see *Open Directory Administration*.

To control access using an access file:

- 1 Use the sudo qtpasswd command-line utility to create user accounts with passwords.
- 2 Create an access file and place it in the media directory you want to protect.
- 3 To disable authentication for a media directory, remove the access file (named qtaccess) or rename it (for example, qtaccess.disabled).

Creating an Access File

An access file is a text file named qtaccess that contains information about users and groups who are authorized to view media in the directory where the access file is stored.

The directory you use to store streamed media can contain other directories, and each directory can have its own access file.

When a user tries to view a media file, the server checks for an access file to see whether the user is authorized to view the media. The server looks first in the directory where the media file is located. If an access file is not found, it looks in the enclosing directory.

The first access file that's found is used to determine whether the user is authorized to view the media file.

The access file for the streaming server works like the Apache web server access file.

You can create an access file with a text editor. The filename must be qtaccess and the file can contain some or all of the following information:

```
AuthName <message>
AuthUserFile <user filename>
AuthGroupFile <group filename>
require user <username1> <username2>
require group <groupname1> <groupname2>
require valid-user
require any-user
```

Terms not in angle brackets are keywords. Anything in angle brackets is information you supply.

Save the access file as plain text (not .rtf or any other file format).

Here's a brief explanation of each keyword:

- `message` is text your users see when the login window appears. It's optional. If your message contains white space (such as a space character between terms), enclose the message in quotation marks.
- `user filename` is the path and filename of the user file. For Snow Leopard, the default is /Library/QuickTimeStreaming/Config/qtusers.
- `group filename` is the path and filename of the group file. For Snow Leopard, the default is /Library/QuickTimeStreaming/Config/qtgroups. A group file is optional. If you have many users, it might be easier to set up groups and then enter the group names, instead of listing each user.
- `username` is a user who is authorized to log in and view the media file. The user's name must be in the user file you specified. You can also specify `valid-user`, which designates any valid user.
- `groupname` is a group whose members are authorized to log in and view the media file. The group and its members must be listed in the group file you specified.

You can use these additional user tags:

- `valid-user` is any user defined in the `qtusers` file. The statement “require valid-user” specifies that any authenticated user in the `qtusers` file can have access to the media files. If this tag is used, the server prompts users for user name and password.
- `any-user` allows any user to view media without providing a name or password.
- `AuthScheme` is a keyword with the values “basic” or “digest” to a `qtaccess` file. This overrides the global authentication setting on a directory-by-directory basis.

If you make customized changes to the default `qtaccess` access file, be aware that making changes to broadcast user settings in Server Admin modifies the default `qtaccess` file at the root level of the `movies` directory. Therefore, customized modifications you make are not preserved.

What Clients Need When Accessing Protected Media

Users must have QuickTime 5 or later to access a media file that digest authentication is enabled for. If your streaming server is set up to use basic authentication, users need QuickTime 4.1 or later.

Users must enter their user names and passwords to view the media file. Users who try to access a media file with an earlier version of QuickTime will see the error message “401: Unauthorized.”

Adding User Accounts and Passwords

You can add a user account and password if you log in to the server computer.

To add a user account:

- 1 Log in to the server computer as root, open a terminal window, and enter the following:

```
sudo qtpasswd <user-name>
```

Alternatively, use `sudo` to execute the command as root.

- 2 Enter a password for the user and reenter it when prompted.

From the command line:

```
#  
# Add a user account.  
# -----  
sudo qtpasswd $USER
```

Adding or Deleting Groups

You can edit the /Library/QuickTimeStreaming/Config/qtgroups file with any text editor as long the file uses this format:

```
<groupname>: <user-name1> <user-name2> <user-name3>
```

For Windows, the path is c:\Program Files\Darwin Streaming Server\qtgroups. For other supported platforms, it is /etc/streaming/qtgroups.

To add or delete a group, edit the group file you set up.

From the command line:

```
# Adding groups:  
echo "$GROUP_NAME: $USER1 $USER2 $USER3" /Library/QuickTimeStreaming/  
Config/qtgroups
```

Making Changes to the User or Group File

You can make changes to the user or group file if you log in to the server computer.

To delete a user from a user or group file:

- 1 Log in to the server computer as administrator and use a text editor to open the user or group file.
- 2 Delete the user name and encrypted passwords line from the user file.
- 3 Delete the user name from the group file.

To change a user password:

- 1 Log in to the server computer as root, open a terminal window, and enter the following:

```
sudo qtpasswd <user-name>
```

Alternatively, use `sudo` to execute the command as root.

- 2 Enter a password for the user.

The password you enter replaces the password in the file.

From the command line:

```
#  
# Change a user password.  
# -----  
sudo qtpasswd $USER
```

Viewing QTSS Logs

QTSS provides the following log files:

- **Error logs.** These log files record errors such as configuration problems. For example, if you bind to a specific IP address that can't be found, or a if user deletes streaming files, these items are logged.
- **Access logs.** When someone plays a movie streamed from your server, the log reports such information as the date, time, and IP address of the computer that played the movie.

QTSS log files are stored in /Library/QuickTimeStreaming/Logs.

QTSS keeps its logs in standard W3C format, allowing you to use a number of popular log analysis tools to parse the data.

To view the QTSS log:

- 1 In Server Admin, click QuickTime Streaming under the server in the Servers list.
- 2 Click Logs and then choose a log from the View pop-up menu.

From the command line:

```
# View the QTSS log:  
sudo tail /Library/QuickTimeStreaming/Logs/$LOG_FILE
```

Use this chapter to learn how to secure Grid and Cluster Computing services.

Protecting grid and cluster services helps control your network's free CPU cycles from misuse. This chapter helps you restrict your network's CPUs to authorized users.

Xgrid, a technology in Snow Leopard Server and Snow Leopard, simplifies deployment and management of computational grids. Xgrid enables you to group computers into grids or clusters, and allows users to easily submit complex computations to groups of computers (local, remote, or both), as an ad hoc grid or a centrally managed cluster.

For more information about configuring multimedia services, see the *Xgrid Administration and High Performance Computing* guide.

Understanding Xgrid Service

Xgrid service handles the transferring of computing jobs to the grid and returns the results. Xgrid does not calculate anything, does not know anything about calculating, does not have content for calculating, and does not even know that you are calculating anything.

The computing job is handled by software (such as perl) that runs on network computers, can be installed before running the computing job, or is transferred to the computers using Xgrid.

The primary components of a computational grid perform the following functions:

- An agent runs one task at a time per CPU. (A dual-processor computer can run two tasks simultaneously.)
- A controller queues tasks, distributes those tasks to agents, and handles task reassignment.
- A client submits jobs to the Xgrid controller in the form of multiple tasks. (A client can be any computer running Tiger or later or Tiger Server or later.)

In principle, the agent, controller, and client can run on the same server, but it is often more efficient to have a dedicated controller node.

Disabling Xgrid Service

If your server is not intended to be an Xgrid server, disable the Xgrid server software. Disabling the software prevents potential vulnerabilities on your computer.

The Xgrid service is disabled by default, but verification is recommended.

To disable Xgrid service:

- 1 Select Xgrid in the Computers & Services list.
- 2 Click Stop Xgrid.
- 3 Click Save.

From the command line:

```
# -----
# Xgrid Service
# -----
#
# Disable Xgrid service.
#
# -----
sudo serveradmin stop xgrid
```

About Authentication Methods for Xgrid

You can configure Xgrid with or without authentication. If you require authentication of controllers to mutually authenticate with clients and agents, you can choose Single Sign-On or Password-Based Authentication.

You set up an Xgrid controller using Server Admin. You can specify the type of authentication for agents and clients. The passwords entered in Server Admin for the controller must match those entered for each agent and client.

When establishing passwords for agents and clients, consider these points:

- **Kerberos authentication (single sign-on).** If you use Kerberos authentication for agents or clients, the server that's the Xgrid controller must be configured for Kerberos, must be in the same realm as the server running the Kerberos domain controller (KDC) system, and must be bound to the Open Directory master.

The agent uses the host principal found in the /etc/krb5.keytab file. The controller uses the Xgrid service principal found in the /etc/krb5.keytab file.

- **Agents.** The agent determines the authentication method. The controller must conform to that method and password (if a password is used). When an agent is configured with a standard password (not single sign-on), you must use the same password for agents when you configure the controller. If the agent has specified single sign-on, the correct service principal and host principals must be available.
- **Clients.** If your server is the controller for a grid, be sure that Snow Leopard and Snow Leopard Server clients use the correct authentication method for the controller.

A client cannot submit a job to the controller unless the user chooses the correct authentication method and enters their password correctly, or has the correct ticket-granting ticket from Kerberos.

For more information, see *Xgrid Administration and High Performance Computing*.

Single Sign-On

Single sign-on (SSO) is the most powerful and flexible form of authentication. It leverages the Open Directory and Kerberos infrastructures in Snow Leopard Server to manage authentication behind the scenes, without user intervention.

Each Xgrid participant must have a Kerberos principal. The clients and agents obtain ticket-granting tickets for their principal, which is used to obtain a service ticket for the controller service principal. The controller looks at the ticket granted to the client to determine the user's principal and verifies it with the relevant service access control lists (SACLs) and groups to determine privileges.

Generally, use this option if any of the following conditions are true:

- You have single sign-on in your environment.
- You have administrator control over all agents and clients in use.
- Jobs must run with special privileges (such as for local, network, or SAN file system access).

Password-Based Authentication

When you can't use single sign-on, you can require password authentication. You may not be able to use single sign-on if:

- Potential Xgrid clients are not trusted by your single sign-on domain (or you don't have one).
- You want to use agents across the Internet or that are outside your control.
- It is an ad hoc grid, without the ability to prearrange a web of trust.

In these situations, your best option is to specify a password. You have two password options: one for controller-client and one for controller-agent. For security reasons, these should be different passwords.

Note: You can also create hybrid environments, such as with client-controller authentication done using passwords but controller-agent authentication done using single sign-on (or vice versa).

No Authentication

The No Authentication method creates potential security risks, because anyone can connect or run a job, which can expose sensitive data. This option is appropriate only for testing a private network in a home or lab that is inaccessible from any untrusted computer, or when none of the jobs or the computers contain sensitive or important information.

Securely Configuring Xgrid Service

Xgrid service must be running for your server to control a grid or participate in a grid as an agent. If Xgrid service is required, configure the Xgrid agent and controller. The Xgrid controller and agent are disabled by default.

When configuring the Xgrid agent and controller, require authentication to protect your network from malicious users. Authentication requires that agent and controller use the same password or authenticate using Kerberos single sign-on. With no authentication, a malicious agent could receive tasks and potentially access sensitive data.

Disabling the Xgrid Agent

An Xgrid agent runs the computational tasks of a job. In Snow Leopard Server, the agent is turned off by default. When an agent is turned on and becomes active at startup, it registers with a controller. (An agent can be connected to only one controller at a time.) The controller sends instructions and data to the agent for the controller's jobs. After it receives instructions from the controller, the agent executes its assigned tasks and sends the results back to the controller.

You use Server Admin to make sure your server is not acting like an Xgrid agent.

To disable an Xgrid agent on the server:

- 1 Select Xgrid in the Computers & Services list.
- 2 Click Settings.
- 3 Click Agent.
- 4 Deselect "Enable agent service."

From the command line:

```
# Configure an Xgrid agent on the server:  
sudo /usr/sbin/xgridctl agent stop  
sudo serveradmin settings xgrid:AgentSettings:Enabled = no
```

Limits the Xgrid Agent

An Xgrid agent registers with a controller and receives instructions and data for the controller's jobs. After it receives instructions from the controller, the agent executes its assigned tasks and sends the results back to the controller.

You use Server Admin to set up your server as an Xgrid agent. In addition, you can associate the agent with a specific controller or permit it to join a grid, specify when the agent accepts tasks, and set a password that the controller must recognize.

To configure an Xgrid agent on the server:

- 1 Open Server Admin and connect to the server.
- 2 Select Xgrid in the Computers & Services list.
- 3 Click Settings.
- 4 Click Agent.
- 5 Click "Enable agent service."
- 6 Specify a controller by choosing its name in the Controller pop-up menu or by entering the controller name.

By default, the agent uses the first available controller.

Note: An agent can find a controller in one of three ways: a specific hostname or IP address, the first available controller that advertises on Bonjour on the local subnet, or by a specific Bonjour service name.service lookup against the domain name server for _xgrid._tcp._ip.

- 7 Specify when the agent will accept tasks.

Tasks can be accepted when the computer is idle or always.

A computer is considered idle when it has no mouse or keyboard input and ignores CPU and network activity. If a user returns to a computer that is running a grid task, the computer continues to run the task until it is finished.

- 8 From the pop-up menu, choose one of the following authentication options and enter the password.
 - **Password** requires that the agent and controller use the same password.
 - **Kerberos** uses SSO authentication for the agent's administrator.

- **None** does not require a password for the agent. This option is *not* recommended because it provides no protection from unapproved use of your grid. With no authentication, an unapproved agent could receive tasks and potentially access sensitive data.

9 Click Save.

Important: If you require authentication, the agent and controller must use the same password or must authenticate using Kerberos single sign-on.

From the command line:

```
# Configure an Xgrid agent on the server.
# -----
sudo serveradmin settings xgrid:AgentSettings:prefs:Enabled = yes
sudo serveradmin settings
    xgrid:AgentSettings:prefs:ControllerAuthentication = "Kerberos"
sudo serveradmin settings xgrid:AgentSettings:prefs:ControllerName =
    "$XGRID_CONTROLLER_HOST"
sudo serveradmin settings xgrid:AgentSettings:Enabled = yes
```

Configuring an Xgrid Controller

You use Server Admin to configure an Xgrid controller. When configuring the controller, you can also set a password for any agent using the grid and for any client that submits a job to the grid.

To configure an Xgrid controller:

- 1** Open Server Admin and connect to the server.
- 2** Select Xgrid in the Computers & Services list.
- 3** Click Settings.
- 4** Click Controller.
- 5** Click “Enable controller service.”
- 6** From the Client Authentication pop-up menu, choose one of the following authentication options for clients and enter the password.
 - **Password** requires that the agent and controller use the same password.
 - **Kerberos** uses sign-on authentication for the agent’s administrator.
 - **None** does not require a password for the agent. This option is *not* recommended because it provides no protection from unapproved use of your grid. With no authentication, an unapproved agent could receive tasks and potentially access sensitive data.
- 7** Click Save.

Important: If you require authentication, the agent and controller must use the same password or must authenticate using Kerberos single sign-on.

From the command line:

```
# Configure an Xgrid controller.  
sudo serveradmin settings xgrid:ControllerSettings:Enabled = yes  
sudo serveradmin settings  
    xgrid:ControllerSettings:prefs:ClientAuthentication = Password  
sudo serveradmin settings xgrid:ControllerSettings:ClientPassword =  
    $XGRID_CLIENT_PASS
```

Managing Who Can Obtain Administrative Privileges (sudo)

Use this chapter to restrict administrator access to the sudo command by specifying who can use this command in the sudoers file.

The sudo command gives root user privileges to users specified in the sudoers file. If you're logged in as an administrator user and your username is specified in the /etc/sudoers file, you can use this command.

Managing the sudoers File

Limit the list of administrators allowed to use the sudo tool to those administrators who require the ability to run commands with root user privileges.

To change the /etc/sudoers file:

- 1 Edit the /etc/sudoers file using the visudo tool, which allows for safe editing of the file, then run the following command with root user privileges:

```
sudo visudo
```

- 2 When prompted, enter your administrator password.

There is a timeout value associated with the sudo tool. This value indicates the number of minutes until sudo prompts for a password again.

The default value is 5, which means that after issuing the sudo command and entering the correct password, additional sudo commands can be entered for 5 minutes without reentering the password. This value is set in the /etc/sudoers file.

For more information, see the sudo and sudoers man pages.

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

```
Defaults timestamp_timeout=0
```

- 4 Restrict which administrators are allowed to run the `sudo` tool 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 when an administrator is added to a system, the administrator must be added to the `/etc/sudoers` file as described above if that administrator needs to use the `sudo` tool.

- 5 Save and quit `visudo`.

For more information, see the `pico` and `visudo` man pages.

Use this chapter to control authorization on your system by managing the policy database.

Authorization on Snow Leopard Server is controlled by a policy database. This database is stored in /etc/authorization. The database format is described in comments at the top of that file.

The SecurityAgent plug-in processes requests for authentication by gathering requirements from the policy database (/etc/authorization).

Actions can be successfully performed only when the user has acquired the rights to do so.

Understanding the Policy Database

The policy database is a property list that consists of two dictionaries:

- The rights dictionary
- The rules dictionary

The Rights Dictionary

The rights dictionary contains a set of key/value pairs, called *right specifications*. The key is the *right name* and the value is information about the right, including a description of what the user must do to acquire the right.

The following is an extract from the policy database installed on your system.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC ...>
<plist version="1.0">
<dict>
...
    <key>rights</key>
    <dict>
        <key></key>
        <dict>
```

```

<key>class</key>
<string>rule</string>
<key>comment</key>
<string>Matches otherwise unmatched rights (i.e., is a default).</
string>
<key>rule</key>
<string>default</string>
</dict>
<key>system.device.dvd.setregion.initial</key>
<dict>
<key>class</key>
<string>user</string>
<key>comment</key>
<string>Used by the DVD player to set the region code the first
time. Note that changing the region code after it has been set requires
a different right (system.device.dvd.setregion.change).</string>
<key>group</key>
<string>admin</string>
<key>shared</key>
<true/>
</dict>
...
<key>config.add.</key>
<dict>
<key>class</key>
<string>allow</string>
<key>comment</key>
<string>Wildcard right for adding rights. Anyone is allowed to add
any (non-wildcard) rights.</string>
</dict>
...

```

In this extract from the policy database, there are three rights:

- The right specification with an empty key string is known as the default right specification. To obtain this right a user must satisfy the default rule which, by default on current versions of Mac OS X, is to prove that they are an administrator.
- `system.device.dvd.setregion.initial` controls whether the user is allowed to set the initial region code for the DVD drive. By default, a user must prove that they are an administrator (in group `admin`) to set the DVD region.
- `config.add.` is a wildcard right specification (it ends with a dot) that matches any right whose name starts with the `config.add.` characters. This right controls whether a user can add a right specification to the policy database. By default, any user can add a right specification.

When a program asks for a right, Authorization Services executes the following algorithm:

- 1 It searches the policy database for a right specification whose key matches the right name.
- 2 If that fails, it searches the policy database for a wildcard right specification whose key matches the right name. If multiple rights are present, it uses the one with the longest key.
- 3 If that fails, it uses the default right specification.

After it has found the relevant right specification, Authorization Services evaluates the specification to decide whether to grant the right. In some cases this is easy (in the extract from the policy database above, `config.add.` is always granted), but in other cases it can be more complex (for example, setting the DVD region requires that you enter an administrator password).

Rules

A rule consists of a set of attributes. Rules are preconfigured when Snow Leopard Server is installed, but applications can change them at any time.

The following table describes the attributes defined for rules.

Rule attribute	Generic rule value	Description
key		The key is the name of a rule. A key uses the same naming conventions as a right. Security Server uses a rule's key to match the rule with a right. Wildcard keys end with a ". The generic rule has an empty key value. Any rights that do not match a specific rule use the generic rule.
group	admin	The user must authenticate as a member of this group. This attribute can be set to any one group.
shared	true	If this is set to true, Security Server marks the credentials used to gain this right as shared. Security Server can use any shared credentials to authorize this right. For maximum security, set sharing to false so credentials stored by Security Server for one application are not used by another application.
timeout	300	The credential used by this rule expires in the specified number of seconds. For maximum security where the user must authenticate every time, set the timeout to 0. For minimum security, remove the timeout attribute so the user authenticates only once per session.

There are some specific rules in the policy database for Mac OS X applications. There is also a generic rule in the policy database that the Security Server uses for any right that doesn't have a specific rule.

Managing Authorization Rights

Managing authorization rights involves creating and modifying right and rule values.

Creating an Authorization Right

To authorize a user for specific rights, you must create an authorization right in the `rights` dictionary. Each right consists of the following:

- The name of the right
- A value that contains optional data pertaining to the right
- The byte length of the value field
- Optional flags

The right always matches up with the generic rule unless a new rule is added to the policy database.

Modifying an Authorization Right

To modify a right, change the relevant value in `/etc/authorization` and save the file:

- To lock out all privileged operations not explicitly allowed, change the generic rule by setting the `timeout` attribute to 0.
- To allow privileged operations after the user is authorized, remove the `timeout` attribute from the generic rule.
- To prevent applications from sharing rights, set the `shared` attribute to `false`.
- To require users to authenticate as a member of the `staff` group instead of the `admin` group, set the `group` attribute to `staff`.

Note: There are APIs that you can use for modifying `/etc/authorization`. It's better to use these APIs than to manually change the values.

Example Authorization Restrictions

As an example of how the Security Server matches a right with a rule in the policy database, consider a grades-and-transcripts application.

The application requests the right `com.myOrganization.myProduct.transcripts.create`. Security Server looks up the right in the policy database. Not finding a match, Security Server looks for a rule with a wildcard key set to `com.myOrganization.myProduct.transcripts.`, `com.myOrganization.myProduct.`, `com.myOrganization.`, or `com.`—in that order—checking for the longest match.

If no wildcard key matches, Security Server uses the generic rule.

Security Server requests authentication from the user. The user provides a user name and password to authenticate as a member of the group `admin`. Security Server creates a credential based on the user authentication and the right requested.

The credential specifies that other applications can use it, and Security Server sets the expiration to five minutes.

Three minutes later, a child process of the application starts up. The child process requests the right com.myOrganization.myProduct.transcripts.create.

Security Server finds the credential, sees that it allows sharing, and uses the right. Two and a half minutes later, the same child process requests the right com.myOrganization.myProduct.transcripts.create again, but the right has expired.

Security Server begins the process of creating a credential by consulting the policy database and requesting user authentication.

Use this chapter to learn how to monitor events and logs to help 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 protect your configuration settings. This chapter also discusses antivirus tools, which detect unwanted viruses.

Using Digital Signatures to Validate Applications and Processes

A digital signature uses public key cryptography to ensure the integrity of data. Like traditional signatures written with ink on paper, they can be used to identify and authenticate the signer of the data.

However, digital signatures go beyond traditional signatures in that they can also ensure that the data itself has not been altered. This is like designing a check in such a way that if someone alters the amount of the sum written on the check, an "Invalid" watermark becomes visible on the face of the check.

To create a digital signature, the signer generates a message digest of the data and then uses a private key to sign the digest. The signer must have a valid digital certificate containing the public key that corresponds to the private key. The combination of a certificate and related private key is called an identity.

The signature includes the signed digest and information about the signer's digital certificate. The certificate includes the public key and the algorithm needed to verify the signature.

To verify that the signed document has not been altered, the recipient uses the algorithm to create a message digest and applies the public key to the signed digest. If the two digests prove identical, the message cannot have been altered and must have been sent by the owner of the public key.

To ensure that the person who provided the signature is not only the same person who provided the data but is also who they say they are, the certificate is also signed—in this case by the certificate authority (CA) who issued the certificate.

Signed code uses several digital signatures:

- If the code is universal, the object code for each architecture is signed separately.
- Components of the application bundle (such as the Info.plist file, if there is one) are also signed.

Validating Application Bundle Integrity

To validate the signature on a signed application bundle, use the `codesign` command with the `-v` option.

From the command line:

```
# -----
# Maintaining System Integrity
# -----
# Validate application bundle integrity.
sudo codesign -v $code_path
```

This command checks that the code binaries at `code-path` are signed, that the signature is valid, that sealed components are unaltered, and that the bundle passes basic consistency checks. It does not verify that the code satisfies requirements except its own designated requirement.

To verify a requirement, use the `-R` option. For example, to verify that the Apple Mail application is identified as Mail, signed by Apple, and secured with Apple's root signing certificate, use the following command:

From the command line:

```
# Verify a requirement.
sudo codesign -v -R="identifier com.apple.Mail and anchor apple" /
    Applications/Mail.app
```

Unlike the `-r` option, the `-R` option takes only a single requirement rather than a requirements collection (no => tags). Add additional `-v` options to get details on the validation process.

For more information about signing and verifying application bundle signatures, see *Code Signing Guide* at developer.apple.com/documentation/Security/Conceptual/CodeSigningGuide. For more information about the `codesign` command, see its man page.

Validating Running Processes

You can also use `codesign` to validate the signatures of running processes.

If you pass a number rather than a path to the `verify` option, `codesign` takes the number to be the process ID (pid) of a running process, and performs dynamic validation instead.

Auditing System Activity

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

The audit subsystem allows authorized administrators to create, read, and delete audit information. The audit subsystem creates a log of auditable events and allows the administrator to read all audit information from the records in a manner suitable for interpretation. The default location for these files is the `/var/audit/` folder.

The audit subsystem is controlled by the `audit` utility located in the `/usr/sbin/` folder. This utility transitions the system in and out of audit operation.

The default configuration of the audit mechanism is controlled by a set of configuration files in the `/etc/security/` folder.

If auditing is enabled, the `/etc/rc` startup script starts the audit daemon at system startup. All features of the daemon are controlled by the `audit` utility and `audit_control` file.

Installing Auditing Tools

The Common Criteria Tools disk image (.dmg) file contains the installer for auditing tools. This disk image file is available from the Common Criteria webpage located at www.apple.com/support/security/commoncriteria/.

After downloading the Common Criteria Tools disk image file, copy it to a removable disk, such as a CD-R disc, FireWire disk, or USB disk.

To install the Common Criteria Tools software:

- 1 Insert the disk that contains the Common Criteria Tools disk image file and open the file to mount the volume containing the tools Installer.
- 2 Double-click the CommonCriteriaTools.pkg installer file.
- 3 Click Continue, then proceed through the installation by following the onscreen instructions.
- 4 When prompted to authenticate, enter the user name and password of the administrator account.

From the command line:

```
# Install the common criteria tools software.  
sudo installer -pkg CommonCriteriaTools.pkg -target /
```

Enabling Auditing

Modify the hostconfig file to enable auditing.

To turn auditing on:

- 1 Open Terminal.
- 2 Enter the following command to edit the /etc/hostconfig file.
`sudo pico /etc/hostconfig`
- 3 Add the following entry to the file.
`AUDIT=-YES-`
- 4 Save the file.

Auditing is enabled when the computer starts up.

The following table shows the possible audit settings and what they do.

Parameter	Description
<code>AUDIT=-YES-</code>	Enable auditing; ignore failure.
<code>AUDIT=-NO-</code>	Disable auditing.
<code>AUDIT=-FAILSTOP-</code>	Enable auditing; processes may stop if failure occurs.
<code>AUDIT=-FAILHALT-</code>	Enable auditing; the system halts if failure occurs.

If the `AUDIT` entry is missing from the /etc/hostconfig file, auditing is turned off. A failure is any occurrence that prevents audit events from being logged.

The audit subsystem generates warnings when relevant events such as storage space exhaustion and errors in operation are recognized during audit startup or log rotation. These warnings are communicated to the `audit_warn` script, which can then communicate these events to the authorized administrator.

From the command line:

```
# Enable auditing.  
sudo cp /etc/hostconfig /tmp/test  
  
if /usr/bin/grep AUDIT /etc/hostconfig  
then  
    sudo /usr/bin/sed "/^AUDIT.*//s//AUDIT=-YES-/g" /tmp/test > /etc/  
        hostconfig  
else  
    /bin/echo AUDIT=-YES- >> /etc/hostconfig  
fi
```

Setting Audit Mechanisms

System startup scripts attempt to configure auditing early in the system startup process. After auditing is enabled, the settings for the audit mechanism are set with the `/etc/security/audit_control` configuration file.

Files containing audit settings can be edited with any text editor. Terminal can be used with `pico` or `emacs` text editor tools. For more information about using text editors with Terminal, see the `pico` or `emacs` man page.

Audit flags are defined in terms of audit classes. Audit flags can be for the whole system, or specific flags can be used for a user. Audit flags can include or exclude classes of events from the audit record stream based on the outcome of the event. For example, the outcome could be success, failure, or both.

When a user logs in, the system-wide audit flags from the `audit_control` file are combined with the user-specific audit flags (if any) from the `audit_user` file, and together establish the preselection mask for the user.

The preselection mask determines which events will generate audit records for a user. If the preselection mask is changed, restart the computer to ensure that all components are producing audit events consistently.

Using Auditing Tools

This section describes how to use auditing tools.

Using the audit Tool

Auditing is managed by the `audit` tool. The `audit` tool uses this syntax:

```
audit [-nst] [file]
```

The `audit` tool controls the state of the auditing subsystem. The optional file operand specifies the location of the `audit_control` input file. The default file is `/etc/security/audit_control`.

You can use the following options with the `audit` tool.

Parameter	Description
<code>-n</code>	Forces the audit system to close the existing audit log file and rotate to a new log file in a location specified in the audit control file.
<code>-s</code>	Specifies that the audit system should restart and reread its configuration from the audit control file. A new log file is created.
<code>-t</code>	Specifies that the audit system should terminate. Log files are closed and renamed to indicate the time of the shutdown.

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

Using the `auditreduce` Tool

The `auditreduce` tool enables you to select events that have been logged in audit records. Matching audit records are printed to the standard output in their raw binary form. If no filename is specified, the standard input is used by default.

The `auditreduce` tool follows this syntax:

```
auditreduce [-A] [-a YYYYMMDD[HH[MM[SS]]]] [-b YYYYMMDD[HH[MM[SS]]]] [-c
           flags] [-d YYYYMMDD] [-e euid] [-f egid] [-g rgid] [-r ruid] [-u auid]
           [-j id] [-m event] [-o object=value] [file ...]
```

For more information, see the `auditreduce` man pages.

Parameter	Description
<code>-A</code>	Selects all records.
<code>-a</code> YYYYMMDD [HH[MM[SS]]]	Selects records that occurred on or after the specified date and time.
<code>-b</code> YYYYMMDD [HH[MM[SS]]]	Selects records that occurred before the specified date and time.
<code>-c</code> flags	Selects records matching the given audit classes, specified as a comma-separated list of audit flags.
<code>-d</code> YYYYMMDD	Selects records that occurred on a specified date. Cannot be used with <code>-a</code> or <code>-b</code> option flags.
<code>-e</code> euid	Selects records with the specified effective user.
<code>-f</code> egid	Selects records with the specified effective group.
<code>-g</code> gid	Selects records with the specified real group.
<code>-r</code> ruid	Selects records with the specified real user.

Parameter	Description
-u	auid Selects records with the specified audit ID.
-j	id Selects records having a subject token with matching ID.
-m	event Selects records with the specified event name or number.
-o	object = value file = Selects records containing the specified path name. file ="/usr" matches paths starting with usr. file ="~/usr" matches paths not starting with usr. msgqid = Selects records containing the specified message queue ID. pid = Selects records containing the specified process ID. semid = Selects records containing the specified semaphore ID. shmid = Selects records containing the specified shared memory ID.

To select all records associated with effective user ID root from the audit log /var/audit/20031016184719.20031017122634:

```
auditreduce -e root /var/audit/20031016184719.20031017122634
```

To select all setlogin events from that log:

```
auditreduce -m AUE_SETLOGIN /var/audit/20031016184719.20031017122634:
```

Using the praudit Tool

The praudit tool prints the contents of audit records. Audit records appear in standard output (stdout). If no filename is specified, standard input (stdin) is used.

The praudit tool uses this syntax:

```
praudit [options] audit-trail-file [...]
```

You can use praudit with the following options:

Parameter	Description
-l	Prints the record in the same line. If this option is not specified, every token appears in a different line.
-r	Prints records in their raw format. This option is separate from -s.
-s	Prints the tokens in their short form. Short ASCII representations for record and event type are displayed. This option is separate from -r.
del	Specifies the delimiter. The default delimiter is the comma.

If raw or short form are not specified, tokens are printed in their long form. Events are displayed according to their descriptions given in audit_event, UIDs and GIDs are expanded to their actual ASCII representation, date and time is displayed in standard date format, and so on.

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

Deleting Audit Records

You can clear the audit trail by deleting audit files using the command line.

WARNING: Do not delete the current audit log.

To delete an audit file:

```
sudo rm /var/audit/20031016184719.20031017122634
```

Audit Control Files

The audit system uses the following text files to control auditing and write audit records. The default location for these files is the `/etc/security/` folder.

- `audit_class`—The `audit_class` file contains descriptions of auditable event classes on the system. Each auditable event is a member of an event class. Each line maps an audit event mask (bitmap) to a class and a description.
- `audit_control`—The `audit_control` file contains several audit system parameters. Each line of this file is of the form `parameter:value`. Audit flags are a comma-delimited list of audit classes as defined in the `audit_class` file. Event classes can be preceded by a prefix that changes their interpretation.
- `audit_event`—The `audit_event` file contains descriptions of auditable events on the system. Each line maps an audit event number to a name, a description, and a class. Each event class should have a corresponding entry in the `audit_class` file.
- `audit_user`—The `audit_user` file specifies which audit event classes are to be audited for specific users. If specified, these flags are combined with system wide audit flags in the `audit_control` file to determine which classes of events to audit for a user. These settings take effect when the user logs in. Each line maps a user name to a list of classes that should be audited and a list of classes that should not be audited.
- `audit_warn`—The `audit_warn` file runs when `audited` generates warning messages. The default `audit_warn` is a script whose first parameter is the type of warning. The script appends its arguments to `/etc/security/audit_messages`. Administrators can replace this script with a more comprehensive one that takes different actions based on the type of warning. For example, a low-space warning could result in a mail message being sent to the administrator.

For more information about editing audit control files, see the *Common Criteria Administration* guide at www.apple.com/support/security.

Managing and Analyzing Audit Log Files

If auditing is enabled, the auditing subsystem adds records of auditable events to an audit log file. The name of an audit log file consists of the date and time it was created, followed by a period, and the date and time it was terminated. For example:

20040322183133.20040322184443.

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

The audit subsystem appends records to only one audit log file at a time. The currently active file has a suffix ".not_terminated" instead of a date and time. Audit log files are stored in the folders specified in the audit_control file. The audit subsystem creates an audit log file in the first folder specified.

When less than the minfree amount of disk space is available on the volume containing the audit log file, the audit subsystem:

- 1 Issues an audit_warn soft warning.
- 2 Terminates the current audit log file.
- 3 Creates a new audit log file in the next specified folder.

After all folders specified have exceeded this minfree limit, auditing resumes in the first folder again. However, if that folder is full, an auditing subsystem failure can occur.

You can also choose to terminate the current audit log file and create a new one manually using the audit utility. This action is commonly referred to as "rotating the audit logs."

Use `audit -n` to rotate the current log file. Use `audit -s` to force the audit subsystem to reload its settings from the audit_control file (which also rotates the current log file).

Using Activity Analysis Tools

Snow Leopard Server 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 large amounts of disk space. Additionally, these tools are only effective when other users don't have administrator access. Users with administrator access can edit logs generated by the tool and thereby circumvent the tool.

If your computer contains sensitive data, consider using both auditing and logging tools. By using both types of tools, you can 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 relevant information for reviewing or archiving purposes.

Validating System Logging

Logging is the recording of various events, including changes to service status, processes, and operating system components. Some events are security related, while others are information messages about your computer's activity.

If an unexpected error occurs, you can analyze logs to help determine the cause of the error. For example, 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. Limit the `sudo` commands that individual users are allowed to use. For more information, see "Managing the sudoers File" on page 361.

Use Console to view and maintain log files. Console is located in the /Applications/ Utilities/ folder. Upon starting, the Console window shows the `console.log` file. Click Logs to display a pane that shows other log files on the system in a tree view. The tree view includes folders for services, such as web and mail server software.

In Snow Leopard Server, log files are handled by the BSD subsystem or by a specific application. The BSD subsystem handles most important system logging, while some applications handle their own logging. Like other BSD systems, Snow Leopard Server uses a background process called `syslogd` to handle logging.

A primary 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`. A manual for configuration of this file is available by issuing the command `man syslog.conf` in a Terminal window.

Each line in `/etc/syslog.conf` consists of text containing three types of data: a facility, a priority, and an action.

- Facilities are categories of log messages. Standard facilities include mail, news, user, and kern (kernel). Priorities deal with the urgency of the message. In order from least to most critical, they are debug, info, notice, warning, err, crit, alert, and emerg.
- The priority of the log message is set by the application sending it, not by `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 a remote host.

The following example specifies that for log messages in the category "mail" with a priority of "emerg" or higher, the message is written to the /var/log/mail.log file:

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

The facility and priority are separated by a period, and these are separated from the action by tabs. Wildcards ("*") can also be used in the configuration file.

The following example 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/newsyslog.conf is configured for local logging in the /var/log folder. The computer is set to rotate log files using the periodic launchd job according to time intervals specified in the /etc/newsyslog.conf file.

Rotation entails compressing the current log file, incrementing the integer in the filename of compressed log files, and creating a log file for new messages.

The following table describes the rotation process after two rotations.

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

Log files are rotated by a launchd job, and the rotation occurs if the computer is on when the job is scheduled. By default, log rotation tasks are scheduled between midnight and 1 in the morning, to be as unobtrusive as possible to users. If the system will not be powered on at this time, adjust the settings in /etc/newsyslog.conf.

For information about editing the /etc/newsyslog.conf file, issue the `man 5 newsyslog.conf` command in a Terminal window.

Remote System Logging

Using remote logging in addition to local logging is strongly recommended, because local logs can easily be altered if the system is compromised. Consider the following security issues 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 fill storage space on the logging system, rendering further logging impossible.
- Log files can indicate suspicious activity only if a baseline of normal activity is established, and if the files are regularly monitored for such activity.

If these security issues outweigh the security benefit of remote logging for the network being configured, do not use remote logging.

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 name or IP address of the log server, and making 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`

Viewing Logs in Server Admin

Server Admin provides logging for some services enabled on your server. A filter feature allows you to search through the log for specific information.

To view logs in Server Admin:

- 1 Open Server Admin and connect to the server.
- 2 Click the triangle at the left of the server.
The list of services appears.
- 3 From the expanded Servers list, select a service.
- 4 Click Logs.

Some services have multiple logs associated with them.

From the command line:

```
# View logs in Server Admin.  
# Use tail or more to view the log files.  
# The audit files are individually named based on the date.  
  
sudo /usr/bin/tail $AUDIT_FILE
```

Understanding Passwords and Authentication

Use this appendix to learn the different types of passwords and how they authenticate users.

Passwords are a common method for authenticating. There are several types of services that use passwords to verify the identity of users.

Password Types

Each user account has a password type that determines how the user account is authenticated. In a local directory domain, the standard password type is shadow password.

For user accounts in the LDAP directory of Snow Leopard Server, the standard password type is Open Directory. User accounts in the LDAP directory can also have a password type of crypt password.

Authentication and Authorization

Services such as the login window and Apple file service request user authentication from Open Directory. Authentication is part of the process by which a service determines whether it should grant a user access to a resource. Usually this process also requires authorization.

Authentication proves a user's identity, and authorization determines what the authenticated user is permitted to do. A user typically authenticates by providing a valid name and password. A service can then authorize the authenticated user to access specific resources. For example, file service authorizes full access to folders and files that an authenticated user owns.

You experience authentication and authorization when you use a credit card. The merchant authenticates you by comparing your signature on the sales slip to the signature on your credit card. Then the merchant submits your authorized credit card account number to the bank, which authorizes payment based on your account balance and credit limit.

Open Directory authenticates user accounts, and service access control lists (SACLs) authorize use of services. If Open Directory authenticates you, the SACL for login window determines whether you can log in, the SACL for Apple Filing Protocol (AFP) service determines whether you can connect for file service, and so on.

Some services also determine whether a user can access specific resources. This authorization can require retrieving other user account information from the directory domain. For example, AFP service needs the user ID and group membership information to determine which folders and files the user can read and write to.

Open Directory Passwords

When a user's account has a password type of Open Directory, the user can be authenticated by Kerberos or the Open Directory Password Server. Kerberos is a network authentication system that uses credentials issued by a trusted server.

Open Directory Password Server supports traditional password authentication methods that some clients of network services require.

Kerberos and Open Directory Password Server do not store the password in the user's account. Kerberos and Open Directory Password Server store passwords in secure databases apart from the directory domain, and passwords can never be read. Passwords can only be set and verified.

Malicious users might attempt to log in over the network hoping to gain access to Kerberos and Open Directory Password Server. Open Directory logs can alert you to unsuccessful login attempts.

User accounts in the following directory domains can have Open Directory passwords:

- The LDAP directory of Snow Leopard Server
- The local directory domain of Snow Leopard Server

Note: Open Directory passwords can't be used to log in to Mac OS X v10.1 or earlier. Users who log in using the login window of Mac OS X v10.1 or earlier must be configured to use crypt passwords. The password type doesn't matter for other services. For example, a user of Mac OS X v10.1 could authenticate for Apple file service with an Open Directory password.

Shadow Passwords

Shadow passwords support the same traditional authentication methods as Open Directory Password Server. These authentication methods are used to send shadow passwords over the network in a scrambled form, or *hash*.

A shadow password is stored as several hashes in a file on the same computer as the directory domain where the user account resides. Because the password is not stored in the user account, the password is not easy to capture over the network. Each user's shadow password is stored in a separate file, named a *shadow password file*, and these files are protected so they can be read only by the root user account.

User accounts stored in a computer's local directory domain are the only ones that can have a shadow password. User accounts that are stored in a shared directory can't have a shadow password.

Shadow passwords also provide cached authentication for mobile user accounts. For more information about mobile user accounts, see *User Management*.

Crypt Passwords

A crypt password is stored in a hash in the user account record. This strategy, historically named *basic authentication*, is most compatible with software that needs to access user records directly. For example, Mac OS X v10.1 or earlier expect to find a crypt password stored in the user account.

Crypt authentication supports a maximum password length of eight bytes (eight ASCII characters). If a longer password is entered in a user account, only the first eight bytes are used for crypt password validation. Shadow passwords and Open Directory passwords are not subject to this length limit.

For secure transmission of passwords over a network, crypt supports the DHX authentication method.

Offline Attacks on Passwords

Because crypt passwords are stored in user accounts, they are subject to cracking. User accounts in a shared directory domain are accessible on the network. Anyone on the network who has Workgroup Manager or knows how to use command-line tools can read the contents of user accounts, including the passwords stored in them.

Open Directory passwords and shadow passwords aren't stored in user accounts, so these passwords can't be read from directory domains.

A malicious attacker could use Workgroup Manager or UNIX commands to copy user records to a file. The attacker can transport this file to a system and use various techniques to decode crypt passwords stored in user records. After decoding a crypt password, the attacker can log in unnoticed with a legitimate user name and crypt password.

This form of attack is known as an offline attack, because it does not require successive login attempts to gain access to a system.

Shadow passwords and Open Directory passwords are far less susceptible to offline attacks because they are not stored in user records. Shadow passwords are stored in separate files that can be read only by someone who knows the password of the root user.

Open Directory passwords are stored securely in the Kerberos KDC and in the Open Directory Password Server database. A user's Open Directory password can't be read by other users, not even by a user with administrator rights for Open Directory authentication. (This administrator can change only Open Directory passwords and password policies.)

Password Guidelines

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

Snow Leopard Server supports passwords that contain UTF-8 characters or any NUL-terminated byte sequence.

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 ! or @).
- 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. Longer 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.

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 needing 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.

To create 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" and the last "f" (from "four" and "forth") with "4," and "s" (from "seven") with "7," the sample phrase becomes:

4sa7yaofb4

- 4 Add special characters.

If we add "\$" after "4," and "&" after "7," the sample phrase becomes:

4\$sa7&yaofb4\$

- 5 Make some letters uppercase.

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

4\$S A7&yAOfb4\$

Safely Storing Your Password

If you store your password or the algorithm used to make your password in a safe place, you can 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 inside a locked container. Alternatively, you can store your passwords in your wallet. By keeping your passwords in your wallet, you keep passwords in a safe location that is also convenient.

It is recommended not to 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 you can view and use these passwords.

Because Keychain Access requires that you authenticate to unlock keychains, it is convenient for you and inaccessible to intruders. Store the Keychain Access password in a safe location. For more information, see "Storing Credentials in Keychains" on page 88.

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 when you think your password has been 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. If you do, 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.

Authentication Services

Open Directory offers options for authenticating users whose accounts are stored in directory domains on Snow Leopard Server, including Kerberos and traditional authentication methods that network services require.

Open Directory can authenticate users by:

- Using Kerberos authentication for single sign-on.
- Using traditional authentication methods and a password stored securely in the Open Directory Password Server database.
- Using traditional authentication methods and a shadow password stored in a secure shadow password file for each user.
- Using a crypt password stored directly in the user's account, for backward compatibility with legacy systems.
- Using a non-Apple LDAP server for LDAP bind authentication.

In addition, Open Directory lets you set up a password policy for all users as well as specific password policies for each user, such as automatic password expiration and minimum password length. (Password policies do not apply to administrators, crypt password authentication, or LDAP bind authentication.)

Determining Which Authentication Option to Use

To authenticate a user, Open Directory must determine which authentication option to use—Kerberos, Open Directory Password Server, shadow password, or crypt password. The user's account contains information that specifies which authentication option to use. This information is the *authentication authority attribute*.

Open Directory uses the name provided by the user to locate the user's account in the directory domain. Then Open Directory consults the authentication authority attribute in the user's account and learns which authentication option to use.

You can change a user's authentication authority attribute by changing the password type in the Advanced pane of Workgroup Manager, as shown in the following table.

Password type	Authentication authority	Attribute in user record
Open Directory	Open Directory Password Server and Kerberos	Either or both: <ul style="list-style-type: none">• ;ApplePasswordServer;• ;Kerberosv5;
Shadow password	Password file for each user, readable only by the root user account	Either: <ul style="list-style-type: none">• ;ShadowHash;¹• ;ShadowHash;<list of enabled authentication methods>
Crypt password	Encoded password in user record	Either: <ul style="list-style-type: none">• ;basic;• no attribute at all

¹ If the attribute in the user record is ;ShadowHash; without a list of enabled authentication methods, default authentication methods are enabled. The list of default authentication methods is different for Snow Leopard Server and Snow Leopard.

The authentication authority attribute can specify multiple authentication options. For example, a user account with an Open Directory password type normally has an authentication authority attribute that specifies Kerberos and Open Directory Password Server.

A user account doesn't need to include an authentication authority attribute. If a user's account contains no authentication authority attribute, Snow Leopard Server assumes a crypt password is stored in the user's account. For example, user accounts created using Mac OS X v10.1 or earlier contain a crypt password but not an authentication authority attribute.

Password Policies

Open Directory enforces password policies for users whose password type is Open Directory or shadow password. For example, a user's password policy can specify a password expiration interval. If the user is logging in and Open Directory determines that the user's password has expired, the user must replace the expired password. Then Open Directory can authenticate the user.

Password policies can disable a user account on a specified date, after a number of days, after a period of inactivity, or after a number of failed login attempts. Password policies can also require passwords to be a minimum length, contain at least one letter, contain at least one number, differ from the account name, differ from recent passwords, or be changed periodically.

The password policy for a mobile user account applies when the account is used while disconnected from the network and while connected to the network. A mobile user account's password policy is cached for use while offline. For more information about mobile user accounts, see *User Management*.

Password policies do not affect administrator accounts. Administrators are exempt from password policies because they can change the policies at will. In addition, enforcing password policies on administrators could subject them to denial-of-service attacks.

Kerberos and Open Directory Password Server maintain password policies separately. An Open Directory server synchronizes the Kerberos password policy rules with Open Directory Password Server password policy rules.

Single Sign-On Authentication

Snow Leopard Server uses Kerberos for single sign-on authentication, which relieves users from entering a name and password separately for every service. With single sign-on, a user always enters a name and password in the login window. Thereafter, the user does not need to enter a name and password for Apple file service, mail service, or other services that use Kerberos authentication.

To take advantage of single sign-on, users and services must be Kerberized—configured for Kerberos authentication—and use the same Kerberos Key Distribution Center (KDC) server.

User accounts that reside in an LDAP directory of Snow Leopard Server and have a password type of Open Directory use the server's built-in KDC. These user accounts are configured for Kerberos and single sign-on. The server's Kerberized services use the server's built-in KDC and are configured for single sign-on.

This Snow Leopard Server KDC can also authenticate users for services provided by other servers. Having more servers with Snow Leopard Server use the Snow Leopard Server KDC requires only minimal configuration.

Kerberos Authentication

Kerberos was developed at MIT to provide secure authentication and communication over open networks like the Internet. It's named for the three-headed dog that guarded the entrance to the underworld of Greek mythology.

Kerberos provides proof of identity for two parties. It enables you to prove who you are to network services you want to use. It also proves to your applications that network services are genuine, not spoofed.

Like other authentication systems, Kerberos does not provide authorization. Each network service determines what you are permitted to do based on your proven identity.

Kerberos permits a client and a server to identify each other much more securely than typical challenge-response password authentication methods. Kerberos also provides a single sign-on environment where users authenticate only once a day, week, or other period of time, easing authentication frequency.

Snow Leopard Server offers integrated Kerberos support that virtually anyone can deploy. Kerberos deployment is so automatic that users and administrators might not realize it's deployed.

Mac OS X v10.3 and later use Kerberos when someone logs in using an account set for Open Directory authentication. It is the default setting for user accounts in the Snow Leopard Server LDAP directory. Other services provided by the LDAP directory server, such as AFP and mail service, also use Kerberos.

If your network has other servers with Snow Leopard Server, joining them to the Kerberos server is easy, and most of their services use Kerberos automatically.

Alternatively, if your network has a Kerberos system such as Microsoft Active Directory, you can set up your Snow Leopard Server and Snow Leopard computers to use it for authentication.

Snow Leopard Server and Snow Leopard or later support Kerberos v5.
Snow Leopard Server and Snow Leopard do not support Kerberos v4.

Smart Card Authentication

Smart cards enable you to carry your digital certificates with you. Snow Leopard allows you to use your smart card when an authentication dialog is presented.

This robust, two-factor authentication mechanism complies with Department of Defense Common Access Card, U.S. PIV, Belgium National Identification Card, Japanese government PKI, and Java Card 2.1 standards. Similar to an ATM card and a PIN code, two-factor authentication relies on something you have and something you know. If your smart card is lost or stolen, it cannot be used unless your PIN is also known.

Security Checklist

This appendix contains a checklist of recommended steps required to secure Snow Leopard Server.

This appendix contains action item checklists 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 decision.

Installation Action Items

For details, see Chapter 2, “Installing Snow Leopard Server.”

Action Item	Completed?	Notes
Securely erase the Mac OS X install partition before installation		
Disable the firmware password before installation		
Install Snow Leopard Server using Mac OS Extended disk formatting		
Do not install unnecessary packages		
Do not transfer confidential information in Server Assistant		
Do not connect to the Internet		
Create administrator accounts with difficult-to-guess names		
Create complex passwords for administrator accounts		

Action Item	Completed?	Notes
Do not enter a password-related hint; instead, enter help desk contact information		
Enter correct time settings		
Use an internal Software Update server		
Update system software using verified packages		
Repair disk permissions after installing software or software updates		

Hardware and Core Snow Leopard Server Action Items

For details, see Chapter 3, "Securing System Hardware."

Action Item	Completed?	Notes
Restrict access to rooms that have computers		
Store computers in locked or secure containers when not in use		
Use a password protected screensaver		

Global Settings for Snow Leopard Server Action Items

For details, see Chapter 4, "Securing Global System Settings."

Action Item	Completed?	Notes
Require a firmware password		
Create an access warning for the login window		
Create an access warning for the command line		
Disable fast user switching with non-trusted users or when multiple users access local accounts		

Account Configuration Action Items

For details, see Chapter 5, "Securing Local Server Accounts."

Action Item	Completed?	Notes
Create an administrator account and a standard account for each administrator		
Create a standard or a managed account for each nonadministrator		
Set parental controls for managed accounts		
Restrict the distribution and use of administrator accounts		
Modify the /etc/authorization file to secure directory domain access		
Disable su		
Disable root account		
Restrict sudo users to only being able to access required commands		
Set a strong password policy		
Use Password Assistant to generate complex passwords		
Authenticate using a smart card, token, or biometric device		
Secure the login keychain		
Secure keychain items		
Create specialized keychains for different purposes		
Use a portable drive to store keychains		

System Software Action Items

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

MobileMe Preferences Action Items

For details, see “Securing MobileMe Preferences” on page 96.

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 99.

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

Appearance Preferences Action Items

For details, see “Securing Appearance Preferences” on page 102.

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 103.

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

CDs & DVDs Preferences Actions Items

For details, see “Securing CDs & DVDs Preferences” on page 105.

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 System Preferences		

Exposé & Spaces Preferences Action Items

For details, see “Securing Exposé & Spaces Preferences” on page 115

Action Item	Completed?	Notes
Disable Dashboard		

Date & Time Preferences Action Items

For details, see “Securing Date & Time Preferences” on page 107.

Action Item	Completed?	Notes
Set a 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 109.

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

Display Preferences Action Items

For details, see “Securing Display Preferences” on page 111.

Action Item	Completed?	Notes
Disable display mirroring		

Dock Preferences Action Items

For details, see “Securing Dock Preferences” on page 111.

Action Item	Completed?	Notes
Set the dock to hide when not in use		

Energy Saver Preferences Action Items

For details, see “Securing Energy Saver Preferences” on page 112.

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		

Action Item	Completed?	Notes
Disable “Restart automatically after a power failure” for power settings		
Disable “Restart automatically if the computer freezes” for power settings		

Keyboard and Mouse Preferences Action Items

For details, see “Securing Bluetooth Preferences” on page 103.

Action Item	Completed?	Notes
Turn off Bluetooth		

Network Preferences Action Items

For details, see “Securing Network Preferences” on page 118.

Action Item	Completed?	Notes
Disable unused hardware devices		
Disable IPv6		

Print & Fax Preferences Action Items

For details, see “Securing Print & Fax Preferences” on page 120.

Action Item	Completed?	Notes
Use printers in secure locations only		
Disable printer sharing		
Disable print browsing		
Disable receiving faxes		
Disable sending faxes		

QuickTime Preferences Action Items

For details, see “Securing Security Preferences” on page 122.

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 122.

Action Item	Completed?	Notes
Require a password to wake the computer from sleep or screen saver for each account		

Sharing Preferences Action Items

For details, see “Securing Sharing Preferences” on page 125.

Action Item	Completed?	Notes
Disable Remote Login		
Disable Apple Remote Desktop		
Disable Remote Apple Events		
Rename your computer to a name that does not indicate the purpose of the computer		

Software Update Preferences Action Items

For details, see “Securing Software Update Preferences” on page 126.

Action Item	Completed?	Notes
Set “Check for updates” according to policy		
Disable “Download important updates in the background”		
Manually update using installer packages		
Transfer installer packages from a test computer		
Verify installer packages before installing		

Sound Preferences Action Items

For details, see “Securing Sound Preferences” on page 128.

Action Item	Completed?	Notes
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 129.

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

Spotlight Preferences Action Items

For details, see “Securing Spotlight Preferences” on page 130.

Action Item	Completed?	Notes
Prevent Spotlight from searching confidential folders		

Startup Disk Preferences Action Items

For details, see “Securing Startup Disk Preferences” on page 133.

Action Item	Completed?	Notes
Carefully choose the startup volume		

Time Machine Preferences Action Items

For details, see “Securing Time Machine Preferences” on page 134.

Action Item	Completed?	Notes
Turn Time Machine on		
Select a safe location to store backups in		

Data Maintenance and Encryption Action Items

For details, see Chapter 8, “Securing Data and Using Encryption.”

Action Item	Completed?	Notes
Set global permissions using POSIX or ACLs		
Strip setuid bits		
Secure home directory permissions		
Enable FileVault for every user		
Encrypt portable files		

Action Item	Completed?	Notes
Set global umask by changing NSUmask settings		
Mandate secure erasing of files		
Mandate secret erasing of partitions		
Mandate securely erasing free space		

Account Policies Action Items

Chapter 22, “Securing Network Accounts,” describes how to set up and manage account policies and user accounts, as well as how to configure settings and preferences for clients. Each topic with security-related configuration settings has its own action item checklist.

Share Points Action Items

For details, see Chapter 17, “Securing File Services and Sharepoints.”

Action Item	Completed?	Notes
Enable SSL in Workgroup Manager		
Disable unused share points		
Disable unused sharing protocols		
Restrict share point access		

Account Configuration Action Items

For details, see “Securing Directory Accounts” on page 319.

Action Item	Completed?	Notes
Disallow simultaneous login		
Use an Open Directory password instead of a crypt password		
Enter a disk quota		
Use POP or IMAP for mail, not both		
Use POSIX or ACL permissions to determine group account access		
Restrict access to specific groups by assigning computers to a list		

Action Item	Completed?	Notes
If accounts are stored in a network domain, disable local accounts		
Specify a time interval to update the preferences cache		

Applications Preferences Action Items

For details, see “Managing Applications Preferences” on page 284.

Action Item	Completed?	Notes
Create a list of approved applications that users can open		
Deselect “User can also open all applications on local volumes”		
Deselect “Allow approved applications to launch non-approved applications”		
Deselect “Allow UNIX tools to run”		

Dock Preferences Action Items

For details, see “Managing Dock Preferences” on page 291.

Action Item	Completed?	Notes
Modify the Applications list to include required applications		
Modify the Documents and Folders list to include required documents and folders		
Deselect “Merge with user’s Dock”		
Deselect “My Applications”		
Deselect “Documents”		
Deselect “Network Home”		
Select “Automatically hide and show the Dock”		

Energy Saver Preferences Action Items

For details, see “Managing Energy Saver Preferences” on page 292.

Action Item	Completed?	Notes
Disable sleeping the computer for all power settings		
Deselect “Start up the computer”		

Finder Preferences Action Items

For details, see “Managing Finder Preferences” on page 293.

Action Item	Completed?	Notes
Select “Use normal finder”		
Deselect “Hard Disks”		
Deselect “Removable media (such as CDs)”		
Deselect “Connected Servers”		
Select “Always show file extensions”		
Deselect “Connect to Server”		
Deselect “Go to iDisk”		
Deselect “Go to Folder”		
Deselect “Eject”		
Deselect “Burn Disk”		
Deselect “Restart”		
Deselect “Shut Down”		

Login Preferences Action Items

For details, see “Managing Login Preferences” on page 295.

Action Item	Completed?	Notes
Deselect “Add network home share point”		
Deselect “User may add and remove additional items”		
Deselect “User may press Shift to keep items from opening”		
Do not allow login or logout scripts		
Do not allow LoginHook or LogoutHook scripts		

Action Item	Completed?	Notes
Enter help desk information as the login message		
Display the login window as name and password text fields		
Do not allow Restart or Shut Down buttons to show in the Login Window		
Do not allow password hints		
Deselect "Auto Login Client Setting"		
Deselect "Allow users to log in using 'console.'"		
Deselect "Enable Fast User Switching"		
Deselect "Log out users after # minutes of activity"		

Media Access Preferences Action Items

For details, see "Managing Media Access Preferences" on page 298.

Action Item	Completed?	Notes
Disable unnecessary media		
Deselect "Allow for CDs"		
Deselect "Allow for CD-ROMs"		
Deselect "Allow for DVDs"		
Deselect "Allow for Recordable Disks"		
Deselect "Allow for Internal Disks"		
Deselect "Allow for External Disks"		
Select "Eject all removable media at logout"		

Mobility Preferences Action Items

For details, see “Managing Mobility Preferences” on page 299.

Action Item	Completed?	Notes
Disable mobile account on insecure or infrequently accessed computers		
Use FileVault on every computer with portable home folders		
Deselect “Synchronize account for offline use”		

Network Preferences Action Items

For details, see “Managing Network Preferences” on page 301.

Action Item	Completed?	Notes
Use your organization-controlled proxy servers		
Bypass trusted hosts and domains		
Deselect “Use Passive FTP Mode (PASV)”		

Printing Preferences Action Items

For details, see “Managing Printing Preferences” on page 307.

Action Item	Completed?	Notes
Reduce access to printers		
Deselect “Allow user to modify the printer list”		
Deselect “Allow printers that connect directly to user’s computer”		
If selecting “Allow printers that connect directly to user’s computer”, then select “Require an administrator password”		
Select a printer and select “Require an administrator password”		

Software Update Preferences Action Items

For details, see “Managing Software Update Preferences” on page 308.

Action Item	Completed?	Notes
Designate an internal server to control software updates		

Access to System Preferences Action Items

For details, see “Managing Access to System Preferences” on page 308.

Action Item	Completed?	Notes
Select “Appearance” to appear in the System Preferences preferences		
Select “Dashboard & Exposé” to appear in the System Preferences preferences		
Select “Displays” to appear in the System Preferences preferences		
Select “Dock” to appear in the System Preferences preferences		
Select “Keyboard & Mouse” to appear in the System Preferences preferences		
Select “Security” to appear in the System Preferences preferences		
Select “Universal” to appear in the System Preferences preferences		
Disable widgets for network managed users		

Universal Access Preferences Action Items

For details, see “Managing Universal Access Preferences” on page 309.

Action Item	Completed?	Notes
Deselect “Turn on Zoom”		
Set Sticky Keys to Off		
Deselect “Show pressed keys on screen”		

Certificates Action Items

For details, see “Managing Certificates” on page 163.

Action Item	Completed?	Notes
Obtain certificates to use with SSL-enabled services		
Create a CA to issue certificates		
Create an SSL certificate for distribution		
Create the files and folders needed by SSL		
Export certificate to client computers		

General Protocols and Service Access Action Items

For details, see “Setting General Protocols and Access to Services” on page 176.

Action Item	Completed?	Notes
Configure NTP to use an internal time server		
Disable SNMP		
Enable SSH		
Do not use “server” or your name to identify the server		
Set a correct date and time		
Use a secure internal NTP server for automatic date and time setting		
Use Certificate Manager to create, use, and maintain identities for SSL-enabled services		
Use SACL to restrict access to AFP, FTP, and Windows file services		

Remote Access Services Action Items

For details, see “Securing Remote Access Services” on page 185.

Action Item	Completed?	Notes
Disable root login using SSH		
Modify the /private/etc/ sshd_config file to further secure SSH		
Generate identity key pairs for login authentication		
Configure access for using SSH through Server Admin using SACLs		
Use SFTP instead of FTP		
Disable VPN services		
If using VPN services, enable either or both L2TP and PPTP		
To use SecurID authentication, edit the VPN configuration file manually		
Configure an access warning banner		
Disable Apple Remote Desktop		
Encrypt Observe and Control traffic by setting “Encrypt all network data”		
Encrypt network data during file copy and package installation by setting “Encrypt transfers when using Install Packages”		
Disable Remote Apple Events		

Network and Host Access Services Action Items

“Securing Network Infrastructure Services” on page 198 describes configuration information to secure your network services. Several services are provided to maintain your network. Each service with security-related configuration settings has its own action item checklist.

IPv6 Protocol Action Items

For details, see “Using IPv6 Protocol” on page 198.

Action Item	Completed?	Notes
Enable IPv6		
Configure IPv6 manually or automatically		

DHCP Service Action Items

For details, see “Securing DHCP Service” on page 200.

Action Item	Completed?	Notes
Disable the DHCP service if not required		
If using DHCP, disable DNS, LDAP, and WINS		
Assign static IP addresses		

DNS Service Action Items

For details, see “Securing DNS Service” on page 202.

Action Item	Completed?	Notes
Disable the DNS service		
Allow only one system to act as the DNS server		
Allow recursive queries and zone transfers only from trusted clients, not from external networks.		
Update and audit DNS regularly		
Specify which IP addresses are allowed to request zone transfers		
Configure BIND to respond with something other than the current version		
Limit or disable DNS recursion		

Firewall Service Action Items

For details, see “Configuring the Firewall” on page 213.

Action Item	Completed?	Notes
Create IP address groups		
Configure firewall rules for groups and services		
Configure advanced rules for groups and services		
Enable stealth mode		
Set up logging		

NAT Service Action Items

For details, see “Securing NAT Service” on page 207.

Action Item	Completed?	Notes
Disable NAT service if not required		
Configure NAT service		
If necessary, forward incoming traffic to an IP address		

Bonjour Service Action Items

For details, see “Securing Bonjour (mDNS)” on page 210.

Action Item	Completed?	Notes
Disable Bonjour unless required		
Disable unused services that should not be discovered through Bonjour		

Collaboration Services Action Items

For details, see “Securing iCal Service” on page 222 and “Securing iChat Service” on page 225.

Action Item	Completed?	Notes
Disable iCal service		
Disable iChat service		
If using iChat service, designate domain names to use		

Action Item	Completed?	Notes
Designate a certificate to use		
Monitor communication using iChat service logs		

Mail Service Action Items

For details, see “Securing Mail Service” on page 233.

Action Item	Completed?	Notes
Turn off support for any protocol that is not required		
Use different systems for providing outgoing and incoming mail service		
Enable SSL for the mail server		
Create and install a signed mail certificate for outgoing and incoming mail service protocols		
Use the “require” setting in the SSL support options (recommended)		
Configure SMTP authentication requirements to reduce junk mail		
Create a list of approved host servers to relay mail		
Enable junk mail filtering		
Enable virus filtering		
Update the virus database at least twice a day		
Set up a problem report account		
Disable the SMTP banner		

File Services Action Items

“Securing File Services and Sharepoints” on page 254 describes configuring file sharing services. Each type of file sharing service with security-related configuration settings has its own action item checklist.

Action Item	Completed?	Notes
Disable file sharing services if not required		
Use as few protocols as possible		
Use AFP		
Disable FTP		
Disable NFS		
Disable SMB		

AFP File Sharing Service Action Items

For details, see “Configuring AFP File Sharing Service” on page 258.

Action Item	Completed?	Notes
Disable Bonjour registration		
Disable browsing with AppleTalk		
Disable Guest access		
Disable administrator to masquerade as another user		
Enter “1” for Guest Connections		
Enable access log		
Set frequency of archiving		
Implement settings for idle user		

FTP File Sharing Service Action Items

For details, see “Configuring FTP File Sharing Service” on page 259.

Action Item	Completed?	Notes
If authentication is possible, use SFTP instead of FTP		
Disconnect client after 1 login failure		
Enter a mail address set up to handle FTP administration		
Select Kerberos for access authentication		
Allow a maximum of 1 authenticated user		

Action Item	Completed?	Notes
Enable anonymous access and designate the number of anonymous users		
Disable MacBinary and disk image autoconversion		
Enable "Show Welcome Message"		
Enable "Show Banner Message"		
Log all login attempts		
Set "Authenticated users see:" to FTP root and Share Points		
Designate files to share with anonymous users		
Configure the /Library/FTPServer/Configuration/ftpaccess		

NFS File Sharing Service Action Items

For details, see "Configuring NFS File Sharing Service" on page 262.

Action Item	Completed?	Notes
Use NFS only on a secure LAN or when Apple and Windows file sharing systems are unavailable		
Restrict an NFS share point to those systems that require it		
Make the list of export options as restrictive as possible		

SMB Action Items

For details, see "Configuring SMB File Sharing Service" on page 263.

Action Item	Completed?	Notes
Do not allow guest access		
Enter the maximum number of clients connections expected		
Set "Log Detail" to at least medium		
Deselect Workgroup Master Browser and Domain Master Browser services		
Turn off WINS registration		

Web Service Action Items

For details, see "Securing Web Service" on page 271.

Action Item	Completed?	Notes
Disable web service if not required		
Disable web modules if not required		
Disable web options if not required		
Create or obtain signed certificates for each domain name		
Enable SSL for web service		
If WebDAV is enabled, assign access privileges for the sites and web folders		
Do not allow web content files and folders to be writable by world		
Configure a realm to allow user access to websites		
Allow users to access blogs through an SSL enabled site		

Client Configuration Management Services Action Items

For details, see "Securing Client Configuration Management Services" on page 284.

Action Item	Completed?	Notes
Disable NetBoot and NetBoot disk images		
Use Server Admin to view NetBoot clients and the status of NetBoot service		

Directory Services Action Items

For details, see "Securing Directory Services" on page 324.

Action Item	Completed?	Notes
Configure Open Directory roles		
Configure Kerberos		

Action Item	Completed?	Notes
Set a server outside of directory domains as Standalone Server		
Enable SSL		
Set global password policies		
Set binding policies		
Set security policies for Open Directory		

Print Service Action Items

For details, see “Securing Print Service” on page 337.

Action Item	Completed?	Notes
Use Server Admin to manage print queues and configure settings		
Specify a default LPR queue		

Multimedia Services Action Items

For details, see “Securing Multimedia Services” on page 344.

Action Item	Completed?	Notes
User Server Admin to configure QTSS		
Use secure digest authentication to configure client access to streamed media files		

Grid and Cluster Computing Services Action Items

For details, see “Securing Grid and Cluster Computing Services” on page 354.

Action Item	Completed?	Notes
If possible, use a single sign-on password		
Always require authentication		
Enable Xgrid agent service		
Set a password for Xgrid		
Enable Xgrid controller service		
Set a password for Xgrid controller		

Action Item	Completed?	Notes
Set a password for the server acting as a grid agent		
Set a password for agents to join a grid and clients to submit jobs		

Validating System Integrity Action Items

For details, see “Maintaining System Integrity” on page 368.

Action Item	Completed?	Notes
Install and enable auditing tools		
Configure audit settings		
Configure log files		
Configure local system using syslog.conf		
Enable remote system logging		
Install file integrity tools		
Install antivirus tools		

Scripts

```
# -----
# Securing Firewall Service
# -----
#
# Add Firewall to the services view
# -----
sudo serveradmin settings
    info:serviceConfig:services:com.apple.ServerAdmin.ipfilter:configured =
        yes
# Start Firewall service
# -----
sudo serveradmin start ipfilter

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

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

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

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

# Updating from Internet Software Update Server
# -----
```

```
# Default Settings.  
# The softwareupdate command checks and lists available  
# updates for download. Software Update preferences are set to the  
# command-line equivalent of.  
# sudo softwareupdate --list --schedule on  
  
# Suggested Settings.  
# Download and install software updates:  
sudo softwareupdate --download --all --install  
  
# Available Settings.  
# Use the following commands to view softwareupdate options.  
# sudo softwareupdate -h  
# or  
# man softwareupdate  
  
# Updating Manually from Installer Packages  
# -----  
# Default Settings.  
# None  
  
# Suggested Settings.  
# Download software updates.  
sudo softwareupdate --download --all  
# Install software updates.  
sudo installer -pkg $Package_Path -target /Volumes/$Target_Volume  
  
# Available Settings.  
# Use the following commands to view installer options.  
# sudo installer -h  
# or  
# man installer  
  
# Verifying the Integrity of Software  
# -----  
# Default Settings.  
# None  
  
# Suggested Settings.  
# Use the shal command to display a file's SHA-1 digest.  
# Replace $full_path_filename with the full path filename of the update  
# package or image that SHA-1 digest is being checked for.  
sudo /usr/bin/openssl sha1 $full_path_filename  
  
# Available Settings.  
# Use the following command to view the version of OpenSSL installed on  
# your computer.  
# sudo openssl version  
# Use the following command to view openssl options.  
# man openssl
```

```
# -----
# Protecting System Hardware
# -----
# Securing Wi-Fi Hardware
# -----
# Remove AppleAirport kernel extensions.
sudo srm -r /System/Library/Extensions/IO80211Family.kext

# Remove Extensions cache files.
sudo touch /System/Library/Extensions

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

# Suggested Setting.
# Remove Bluetooth kernel extensions.

# Remove Bluetooth kernel extensions.
sudo srm -r /System/Library/Extensions/IOBluetoothFamily.kext
sudo srm -r /System/Library/Extensions/IOBluetoothHIDDriver.kext

# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings.
# None

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

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

# Available Settings.
# None

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

# Suggested Setting.
# Remove Audio Recording kernel extensions.
sudo srm -rf /System/Library/Extensions/AppleUSBAudio.kext
```

```
sudo srm -rf /System/Library/Extensions/IOAudioFamily.kext
# Remove Extensions cache files.
sudo touch /System/Library/Extensions

# Available Settings.
# None

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

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

# Available Settings.
# None

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

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

# Available Settings.
# None

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

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

```

# Available Settings.
# None

# Securing Global System Settings
# -----
# Configuring Firmware Settings
# -----
# Default Setting.
# security-mode is off

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

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

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

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

# -----
# Securing System Preferences
# -----
# Securing MobileMe Preferences
# -----
# Default Setting.
# If a MobileMe account is entered during setup, MobileMe is configured
# for that account.
# Use the following command to display current MobileMe settings.

```

```

# defaults -currentHost read com.apple.<PreferenceIdentifier>
# Use the following command to view all current settings for currenHost.
# defaults -currentHost read

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

# Available Settings.
# None

# Securing Accounts Preferences
# -----
# Change an account's password on a client system.
# Don't use this command if other users are also logged in.
sudo dscl /LDAPv3/127.0.0.1 passwd /Users/$User_name $Oldpass $Newpass

# Change an account's password on a server.
# Don't use this command if other users are also logged in.
sudo dscl . passwd /Users/$User_name $Oldpass $Newpass

# Make sure there is no password hint set.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    RetriesUntilHint -int 0

# Disable Show the Restart, Sleep, and ShutDown Buttons.
sudo defaults write /Library/Preferences/com.apple.loginwindow
    PowerOffDisable -bool yes

# Disable fast user switching. This command does not prevent multiple users
# from being logged in.
sudo defaults write /Library/Preferences/.GlobalPreferences
    MultipleSessionEnabled -bool NO
# Disable Automatic login.
sudo defaults write /Library/Preferences/.GlobalPreferences\
com.apple.userspref.DisableAutoLogin -bool yes

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

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

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

```

```

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

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

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

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

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

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

```

```

# action 107 = "Open iPhoto"
# action 109 = "Open Front Row"

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

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

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

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

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

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

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

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

# Available Settings.

```

```

# autohide -bool YES
# autohide -bool NO

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

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

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

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

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

# Available Settings.
# Enabled or Disabled

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

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

# Available Settings.
# Bluetooth Sharing.
# Disabled
# Enabled

# Securing Network Preferences
# -----

```

```

# Default Setting.
# Enabled

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

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

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

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

# Available Settings.
# Enabled or Disabled

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

# Suggested Setting.
# Enable Require password to wake this computer from sleep or screen saver.
sudo defaults -currentHost write com.apple.screensaver askForPassword -int 1
# Disable IR remote control.
sudo defaults write /Library/Preferences/com.apple.driver.AppleIRController
    DeviceEnabled -bool no
# Enable FileVault.
# To enable FileVault for new users, use this command.
sudo /System/Library/CoreServices/ManagedClient.app/Contents/Resources/\

```

```

createmobileaccount
# Enable Firewall.
# Replace value with
# 0 = off
# 1 = on for specific services
# 2 = on for essential services
sudo defaults write /Library/Preferences/com.apple.alf globalstate -int
    value

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

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

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

# Securing Software Updates Preferences
# -----
# Default Setting.
# Check for Updates: Enabled
# Check Updates: Weekly

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

# Available Setting.
# Startup Disk = Valid Boot Volume

```

```

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

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

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

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

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

# Available Setting.
# None

#
# Securing System Swap and Hibernation Storage
# -----
# Enable secure virtual memory.
sudo defaults write /Library/Preferences/com.apple.virtualMemory \
    UseEncryptedSwap -bool YES

# Restart to take effect.
# sudo shutdown -r now

#
# Using Disk Utility to Securely Erase Free Space
# -----
# Overwrite a device with zeroes.
sudo diskutil zeroDisk /dev/device

# Secure erase (7-pass) free space on a volume.
sudo diskutil secureErase freespace 2 /dev/device

# Secure erase (7-pass) a volume.
sudo diskutil secureErase 2 /dev/device

#
# Adding the security tool edit trust settings

```

```

# -----
# Where <certificate> is the local file path to the certificate.
#
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/
    System.keychain <certificate>

# -----
# Setting General Protocols
# -----


#
# Disable NTP Client access.
#
# -----
sudo systemsetup -setusingnetworktime off

#
# Disable NTP service.
#-----
sudo serveradmin settings info:ntpTimeServe = no

#
# Disable SNMP.
# -----
sudo serveradmin settings info:enableSNMP = no

# or alternatively.
#sudo service org.net-snmp.snmpd stop

#
# Enable SSH.
# -----
sudo service ssh start

# or alternatively.
# sudo serveradmin settings info:enableSSH = yes

#
# Remote Management (ARD)
# -----
# Limiting Remote Management Access
# Repeat for each specified user.
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
    Resources/kickstart -activate -configure -access -on -users
        $ARD_USERNAME -privs -
            <none|all|ControlObserve|DeleteFiles|ControlObserve|TextMessages|ShowOb
                serve|OpenQuitApps|GenerateReports|RestartShutDown|SendFiles|ChangeSett
                    ings|ObserveOnly> -restart
# Specify the user
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
    Resources/kickstart -allowAccessFor -specifiedUsers $ARD_USERNAME

```

```

#
## Disable Remote Management
# -----
# To remove user access:
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
    Resources/kickstart -activate -configure -access -off

# To stop the ARD agent:
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/
    Resources/kickstart -agent -stop

# To disable the service:
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/\
    Resources/kickstart -deactivate -stop

#or alternatively.
# sudo serveradmin settings info:enableARD = no

#
# Remote Apple Events (RAE)
# -----
# Disable Remote Apple Events.
sudo launchctl unload -w /System/Library/LaunchDaemons/eppc.plist

# Set SACL permissions for a service.
# -----
sudo dseditgroup -o edit -a $USER -t user $SACL_GROUP

# -----
# Enabling IPv6
# -----


# Enable IPv6.
# -----
sudo networksetup -setv6on [networkservice]

# -----
# Securing DHCP Service
# -----


# Disable DHCP Service
# -----
sudo serveradmin stop dhcp

# Configuring DHCP Services
# -----
# Set a DHCP subnet's DNS, LDAP, and WINS parameters to no value
sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:dhcp_domain_name_serve
    r:_array_index:0 = ""

```

```

sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:dhcp_ldap_url:_array_i
    ndex:0 = -empty_array
sudo serveradmin set
    dhcp:configuration:subnets:_array_id:$SUBNET_GUID:WINS_node_type =" NOT
    SET"

# Set a DHCP client's static IP address
# -----
# Each computer needs its own GUID within the static map array.
# Increment the array index value for network interfaces
# for a single computer.
serveradmin settings
    dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:ip_address:_array_in
    dex:0 = $ASSIGNED_IP_ADDRESS
serveradmin settings
    dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:en_address:_array_in
    dex:0 = $COMPUTER_MAC_ADDRESS
serveradmin settings dhcp:static_maps:_array_id:$GUID_FOR_STATIC_CLIENT:name
    = $COMPUTER_NAME
# -----
# Securing DNS Service
# -----

# Disable DNS Service.
# -----
sudo serveradmin stop dns

# -----
# Securing NAT Service
# -----

# Disable NAT service.
# -----
sudo serveradmin stop nat

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

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

# -----
# Securing Firewall Service

```

```

# -----
# Start firewall service.
# -----
sudo serveradmin start ipfilter

# Enable stealth mode.
# -----
sudo serveradmin settings ipfilter:blackHoleTCP = true
sudo serveradmin settings ipfilter:blackHoleUDP = true

# View the firewall service log.
# -----
sudo tail /var/log/ipfw.log

# -----
# Securing Collaboration Services
# -----


# -----
# Securing iCal service
# -----


# Disable iCal service.
# -----
sudo serveradmin stop calendar

# Choose an authentication method for iCal service.
# -----
# To enable all auth methods:
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
sudo serveradmin stop calendar; sudo serveradmin start calendar

# To choose Digest auth only:
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "no"
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "yes"
sudo serveradmin stop calendar; sudo serveradmin start calendar

# For Kerberos only:
sudo serveradmin settings calendar:Authentication:Kerberos:Enabled = "yes"
sudo serveradmin settings calendar:Authentication:Digest:Enabled = "no"
sudo serveradmin stop calendar; sudo serveradmin start calendar

# Enable secure network traffic using SSL transport.
# -----
sudo serveradmin settings calendar:SSLPort = 8443

# View the iCal service log
# -----
sudo tail /var/log/caldavd/access.log

```

```

# Disable iChat service.
# -----
sudo serveradmin stop jabber

# Securely configure iChat service.
# To select an iChat server certificate:
sudo serveradmin settings jabber:sslKeyFile = "/etc/certificates/
    Default.crtkey"

# (Or replace the path with the full path to the certificate that you want
# to select.)
# Restart the service if it is running:
sudo serveradmin stop jabber; sudo serveradmin start jabber

# To select an iChat server auth method use one of the following:
sudo serveradmin settings jabber:authLevel = "ANYMETHOD"
sudo serveradmin settings jabber:authLevel = "KERBEROS"
sudo serveradmin settings jabber:authLevel = "STANDARD"

# Then restart the service:
sudo serveradmin stop jabber
sudo serveradmin start jabber

#
# Select a certificate.
# -----
sudo serveradmin settings jabber:sslKeyFile = "/etc/certificates/
    Default.crtkey"

# View the iChat service log.
# -----
sudo tail /var/log/server.log | grep jabberd

# -----
# Securing Wiki Service
# -----



# Disable Wiki service.
# -----
sudo serveradmin stop teams

#
# View the wiki service log.
# -----
sudo tail /Library/Logs/wikid/access.log

# -----
# Securing Podcast Producer Service
# -----

```

```

# Disable Podcast Producer service.
#
# -----
sudo serveradmin stop pcast

#
# View the Podcast Producer service log.
# -----
sudo tail /Library/Logs/pcastserverd/pcastserverd_out.log

# -----
# Securing Mail Service
# -----


# Disable mail service protocols
sudo serveradmin settings mail:imap:enable_pop = no
sudo serveradmin settings mail:imap:enable_imap = no
sudo serveradmin settings mail:postfix:enable_smtp = no

# Set the POP authentication method:
sudo serveradmin settings mail:imap:pop_auth_apop = no
sudo serveradmin settings mail:imap:pop_auth_clear = no
sudo serveradmin settings mail:imap:pop_auth_gssapi = no

# Set SSL transport for POP connections:
sudo serveradmin settings mail:imap:tls_server_options = "use"

# Set secure IMAP authentication:
sudo serveradmin settings mail:imap:imap_auth_login = no
sudo serveradmin settings mail:imap:imap_auth_plain = no
sudo serveradmin settings mail:imap:imap_auth_gssapi = no
sudo serveradmin settings mail:imap:imap_auth_clear = no
sudo serveradmin settings mail:imap:imap_auth_cram_md5 = no

# Configure SSL transport for IMAP connections (same as POP)
sudo serveradmin settings mail:imap:tls_server_options = "use"

# Allow secure SMTP authentication:
sudo serveradmin settings mail:postfix:smtpd_sasl_auth_enable = yes
sudo serveradmin settings mail:postfix:smtpd_use_pw_server = "yes"
sudo serveradmin settings
    mail:postfix:smtpd_pw_server_security_options:_array_index:0 = "gssapi"
sudo serveradmin settings
    mail:postfix:smtpd_pw_server_security_options:_array_index:1 = "cram-
        md5"
sudo serveradmin settings
    mail:postfix:smtpd_pw_server_security_options:_array_index:2 = "login"
sudo serveradmin settings
    mail:postfix:smtpd_pw_server_security_options:_array_index:3 = "plain"

# Configure SSL transport for SMTP connections:
sudo serveradmin settings mail:postfix:smtpd_use_tls = "yes"

```

```

# Enable a user's mail access using ACLs
sudo dseditgroup -o edit -a $USER -t user com.apple.access_mail

# Restrict SMTP relay:
sudo serveradmin settings mail:postfix:mynetworks_enabled = yes

# Reject unauthorized SMTP connections:
sudo serveradmin settings mail:postfix:smtp_reject_list_enabled = yes
sudo serveradmin settings mail:postfix:smtp_reject_list:_array_index:0 =
    "$NETWORK"

# Reject mail from blacklisted senders:
sudo serveradmin settings mail:postfix:black_hole_domains:_array_index:0 =
    "$BLACKLIST_SERVER"
sudo serveradmin settings mail:postfix:maps_rbl_domains_enabled = yes

# Enable junk mail screening:
sudo serveradmin settings mail:postfix:spam_scan_enabled = yes

# Train the filter:
sudo sa-learn --showdots --spam $JUNK_DIRECTORY/*
sudo sa-learn --showdots --ham $NON_JUNK_DIRECTORY/*

# Automatically train the junk mail filter:
sudo /etc/mail/spamassassin/learn_junk_mail

# Allow mail by language and locale:
sudo serveradmin settings mail:postfix:spam_ok_languages = "en fr de"
sudo serveradmin settings mail:postfix:spam_ok_locales = "en"

# Enable virus screening:
sudo serveradmin settings mail:postfix:virus_scan_enabled = yes

# View a mail service log:
sudo tail /var/log/mail.log

# -----
# Securing Antivirus Services
# -----


# Enable virus screening
sudo serveradmin settings mail:postfix:virus_scan_enabled = yes

# View a virus log:
sudo tail /var/log/amavisd.log

# -----
# Securing File Services
# -----

```

```

# Disable file sharing services.
sudo serveradmin stop afp
sudo serveradmin stop smb
sudo serveradmin stop ftp
sudo serveradmin stop nfs

# Securely configure AFP service:
sudo serveradmin settings afp:registerNSL = no
sudo serveradmin settings afp:attemptAdminAuth = no
sudo serveradmin settings afp:clientSleepOnOff = no
sudo serveradmin settings afp:idleDisconnectOnOff = yes
sudo serveradmin settings afp:authenticationMode = "kerberos"
sudo serveradmin settings afp:activityLog = yes
sudo serveradmin settings afp:guestAccess = no

# Configure FTP to provide anonymous FTP downloads:
sudo serveradmin settings ftp:logSecurity:anonymous = yes
sudo serveradmin settings ftp:logSecurity:guest = yes
sudo serveradmin settings ftp:logSecurity:real = yes
sudo serveradmin settings ftp:maxRealUsers = 1
sudo serveradmin settings ftp:enableMacBinAndDmgAutoConversion = no
sudo serveradmin settings ftp:authLevel = "KERBEROS"
sudo serveradmin settings ftp:anonymousAccessPermitted = yes
sudo serveradmin settings ftp:bannerMessage = "$BANNER"
sudo serveradmin settings ftp:maxAnonymousUsers = 500
sudo serveradmin settings ftp:administratorEmailAddress = "user@domain.com"
sudo serveradmin settings ftp:logCommands:anonymous = yes
sudo serveradmin settings ftp:logCommands:guest = yes
sudo serveradmin settings ftp:logCommands:real = yes
sudo serveradmin settings ftp:loginFailuresPermitted = 1
sudo serveradmin settings ftp:welcomeMessage = "$WELCOME"

# Securely configure Windows file sharing service
sudo serveradmin settings smb:wins support = no
sudo serveradmin settings smb:domain master = no
sudo serveradmin settings smb:map to guest = "Never"
sudo serveradmin settings smb:auth methods = "odSAM"
sudo serveradmin settings smb:ntlm auth = "no"
sudo serveradmin settings smb:max smbd processes = 1000
sudo serveradmin settings smb:log level = 1
sudo serveradmin settings smb:preferred master = no
sudo serveradmin settings smb:os level = 65

# -----
# Securing Web Service
# -----


# Disable web service:
sudo serveradmin stop web

# Disable web options:

```

```

sudo serveradmin settings web:Modules:_array_id:authz_host_module:enabled =
    no
sudo serveradmin settings web:Modules:_array_id:dav_module:enabled = no
sudo serveradmin settings web:Modules:_array_id:dav_fs_module:enabled = no
sudo serveradmin settings
    web:Modules:_array_id:apple_spotlight_module:enabled = no
sudo serveradmin settings web:Sites:_array_id:$SITE:SpotlightIndexing = no
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
    Library/WebServer/Documents:AllowOverride = "None"
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
    Library/WebServer/Documents:IfModule:_array_id:mod_dav.c:DAV = no
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
    Library/WebServer/Documents:Options:Includes = no
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
    Library/WebServer/Documents:Options:ExecCGI = no
sudo serveradmin settings web:Sites:_array_id:$SITE:Directory:_array_id:/
    Library/WebServer/Documents:Options:Indexes = no
sudo serveradmin settings
    web:Sites:_array_id:default_default:SpotlightIndexing = no

#
# Configure Apache to prompt you for a passphrase when it starts.
#-----
sudo serveradmin settings web:IfModule:_array_id:mod_ssl.c:SSL
    PassPhraseDialog=builtin

#
# View logs.
#-----
sudo tail /var/log/apache2/access_log

#
# Disable blog service.
#-----
sudo serveradmin settings web:Sites:_array_id:$SITE: weblog = no

# -----
# Securing Tomcat
# -----
# Stop Tomcat using Server Admin:
sudo /Library/Tomcat/bin/startup.sh stop

# -----
# Securing MySQL
# -----
# Turn MySQL service off
sudo serveradmin stop mysql

#

```

```

# Configure MySQL service settings.
# -----
sudo serveradmin settings mysql:allowNetwork = no

#
# View MySQL service logs.
# -----
sudo tail /Library/Logs/MySQL.log

# Securing Client Configuration Management Services
# =====
# If the intended target is a client system, the target for the dscl
# commands should be "/LDAPv3/127.0.0.1". If the management target is the
# server itself, the target should be ".".

# Disable Front Row:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.frontrow
    PreventActivation always -bool 1

# Setting up a list of accessible applications
# -----
# Allow access to applications stored on the user's local hard disk:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess OpenItemsInternalDrive always -bool 1

# Allow helper applications:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess ApprovedAppLaunchesOthers always -bool 1

# Allow UNIX tools:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.applicationaccess AllowUnbundledApps always -bool 1

# Managing Dock Preferences
# -----
# Set Dock hiding
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock autohide-
    immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.dock autohide
    always -bool 1

# Managing Finder Preferences
# -----
# Manage Finder preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    AppleShowAllExtensions-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitBurn always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitConnectTo always -bool 1

```

```

sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitEject always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitGoToFolder always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ProhibitGoToDisk always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowHardDrivesOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowMountedServersOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER com.apple.finder
    ShowRemovableMediaOnDesktop-immutable always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
    AppleShowAllExtensions always -bool 1

# Managing Login Preferences
# -----
# Manage login preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow LoginwindowText always -string
        "$LOGIN_WINDOW_MESSAGE"
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow mcx_UseLoginWindowText always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow RestartDisabled always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow ShutDownDisabled always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow SHOWFULLNAME always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.loginwindow DisableConsoleAccess always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER .GlobalPreferences
    MultipleSessionEnabled always -bool 0

# Managing Network Preferences
# -----
# Manage network preferences:
sudo networksetup -setwebproxystate Ethernet on
sudo networksetup -setwebproxy Ethernet "http://$SERVER" 8008

sudo networksetup -setpassiveftp Ethernet on

# Managing Parental Control Preferences
# -----
# Hide profanity:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.Dictionary
    parentalControl always -bool 1

# Managing Printing Preferences
# -----
# Manage printing preferences:

```

```

sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
    RequireAdminToAddPrinters always -bool 1
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER com.apple.mcxprinting
    AllowLocalPrinters always -bool 0

# Managing Software Update Preferences
# -----
# Manage Software Update preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Computers/$COMPUTER
    com.apple.SoftwareUpdate CatalogURL always -string "http:$SERVER:8088/
index.sucatalog"

# Managing Universal Access Preferences
# -----
# Manage Universal Access preferences:
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKey always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKeyBeepOnModifier always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess stickyKeyShowWindow always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess closeViewDriver always -bool 0
sudo dscl /LDAPv3/127.0.0.1 mcxset /Users/$USER -v 2
    com.apple.universalaccess closeViewShowPreview always -bool 0

# -----
# Securing NetBoot Service
# -----
#
# Disable NetBoot.
sudo serveradmin stop netboot

#
# Securely configure NetBoot.

#
# View NetBoot service logs.
sudo tail /var/log/system.log | grep bootpd

# -----
# Securing Software Update Service
# -----


# Disable Software Update:
sudo serveradmin stop swupdate

#
# Specify which client can access software updates.
# -----
sudo serveradmin settings swupdate:autoEnable = no

```

```

#
# View Software Update service logs.
#
# -----
sudo tail /var/log/swupd/swupd_*

#
# Securing Directory Services
#
# -----


# Configure the Open Directory role:
sudo slapconfig -createldapmasterandadmin $ADMIN $ADMIN_FULL_NAME $ADMIN_UID
$SEARCH_BASE $REALM

# Start Kerberos manually on an Open Directory master:
sudo kdcsetup -a $ADMIN $REALM

#
# Change the global password policy of user accounts in the same domain.
#
# -----
sudo pwpolicy -a $ADMIN_USER -setglobalpolicy "usingHistory=3 requiresAlpha
requiresNumeric maxMinutesUntilChangePassword=131487 minChars=12
maxFailedLoginAttempts=3"

#
# Set the binding policy for an Open Directory master.
#
# -----
sudo slapconfig -setmacosxodpolicy -binding required

#
# Set the security policy for an Open Directory master.
#
# -----
sudo slapconfig -setmacosxodpolicy -cleartext blocked -encrypt yes
-sign yes -man-in-the-middle blocked -clientcaching no

#
# Securing RADIUS Service
#
# -----


# Disable RADIUS
sudo serveradmin stop radiusc

# Use a custom certificate:
sudo serveradmin settings radius:eap.conf:CA_file = "/etc/certificates/
$CA_CRT"
sudo serveradmin settings radius:eap.conf:private_key_file = "/etc/
certificates/$KEY"
sudo serveradmin settings radius:eap.conf:private_key_password = "$PASS"
sudo serveradmin settings radius:eap.conf:certificate_file = "/etc/
certificates/$CERT"

```

```

#
# Edit RADIUS access.
#
# -----
sudo dseditgroup -o edit -a $USER -t user com.apple.access_radius

#
# View the RADIUS log
#
# -----
sudo tail /var/log/radius/radius.log

#
# -----
# Securing Print Service
#
# -----
#
# Disable print service.
#
# -----
sudo serveradmin stop print

# Set administrator SACL permissions for print service:
sudo dseditgroup -o edit -a $USER -t user com.apple.monitor_print

#
# Configure Kerberos for print service.
#
# -----
sudo serveradmin settings sudo serveradmin settings print:authType =
KERBEROS

#
# Configure a Print queue.
#
# -----
sudo serveradmin settings print:lprQueues:_array_index:0 =
$PRINTER_SHARING_NAME
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:sharingName =
$PRINTER_SHARING_NAME
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:quotasEnforced = yes
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:showNameInBonjour = no
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:defaultCoverPage = "classified"
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:sharingList:_array_index:0:serv
ice = "IPP"
sudo serveradmin settings
    print:queuesArray:_array_id:example_com:sharingList:_array_index:0:shar
ingEnable = yes
sudo serveradmin settings print:queuesArray:_array_id:example_com:printerURI =
"lpd://example.com"
sudo serveradmin settings print:queuesArray:_array_id:example_com:shareable =
yes

```

```

sudo serveradmin settings
    print:queuesArray:_array_id:example_com:printerName = "example_com"
sudo serveradmin settings print:useRemoteQueues = yes
sudo serveradmin settings print:coverPageNames:_array_index:0 = "classified"

#
# View print service logs.
# -----
sudo tail /Library/Logs/PrintService/PrintService_admin.log

# -----
# Securing Multimedia Services
# -----
#
# Disable QTSS.
# -----
sudo serveradmin stop qtss

#
# Configure a streaming server.
# -----
sudo serveradmin settings qtss:server:bind_ip_addr:_array_index:0 =
    "$BIND_IP_ADDRESS"

# Serve QuickTime streams over HTTP port 80:
sudo serveradmin settings qtss:server:rtsp_port:_array_index:0 =
    554qtss:server:rtsp_port:_array_index:1 =
    80qtss:server:rtsp_port:_array_index:2 =
    8000qtss:server:rtsp_port:_array_index:3 = 8001

# Change the MP3 broadcast password:
sudo serveradmin settings
    qtss:modules:_array_id:QTSSMP3StreamingModule:mp3_broadcast_password =
        "$QTMP3_PASSWORD"

#
# Create a broadcast user name and password on the streaming server.
# -----
sudo serveradmin settings
    qtss:modules:_array_id:QTSSReflectorModule:allow_broadcasts = yes

#
# Add a user account.
# -----
sudo qtpasswd $USER

# Adding groups:
echo "$GROUP_NAME: $USER1 $USER2 $USER3" /Library/QuickTimeStreaming/Config/
    qtgroups

#

```

```

# Change a user password.
# -----
sudo qtpasswd $USER

# View the QTSS log:
sudo tail /Library/QuickTimeStreaming/Logs/$LOG_FILE

# -----
# Xgrid Service
# -----
#
# Disable Xgrid service.

# Configure an Xgrid agent on the server:
sudo /usr/sbin/xgridctl agent stop

# Configure an Xgrid agent on the server.

# Configure an Xgrid controller.
sudo serveradmin settings xgrid:ControllerSettings:Enabled = yes
sudo serveradmin settings
    xgrid:ControllerSettings:prefs:ClientAuthentication = Password
sudo serveradmin settings xgrid:ControllerSettings:ClientPassword =
    $XGRID_CLIENT_PASS

# -----
# Maintaining System Integrity
# -----


# Validate application bundle integrity.
sudo codesign -v $code_path

# Verify a requirement.
sudo codesign -v -R="identifier com.apple.Mail and anchor apple" /
    Applications/Mail.app

# Install the common criteria tools software.
sudo installer -pkg CommonCriteriaTools.pkg -target /

# Enable auditing.
sudo cp /etc/hostconfig /tmp/test

if /usr/bin/grep AUDIT /etc/hostconfig
then
    sudo /usr/bin/sed "/^AUDIT.*//s//AUDIT=-YES-/g" /tmp/test > /etc/hostconfig
else
    /bin/echo AUDIT=-YES- >> /etc/hostconfig
fi

# View logs in Server Admin.
# Use tail or more to view the log files.

```

```
# The audit files are individually named based on the date.  
sudo /usr/bin/tail $AUDIT_FILE
```

Index

A

access

ACLs 183, 240, 381
application 284, 285, 289
connection control 241–245
Directory Access 320
file 349
media 299
passwords 348, 351
playlists 349
printing 338
QTSS 347, 348, 349, 353
restricting NetBoot 313
restricting Software Update 316
SACLs 183, 228
share point 264–268
Universal Access 309–310
user 30–33, 274, 348, 349, 351
weblogs 280–281
website 274, 302–304
wireless users 333
See also ACLs; IMAP; LDAP; permissions

access control lists. *See* ACLs

access warnings 65–69

See also permissions

accounts

administrator 71–72, 76–81, 319
authentication 349
authentication setup 84–94
creating secure 74–81
credential storage 88–93
directory domains 81–84
group 321–322, 352
mobile 82, 299–301
nonadministrator user 71–72
preferences 99–101
types 71
user 351, 352
See also user accounts; Workgroup Manager

ACEs (access control entries) 144

Acknowledgments 23

ACLs (access control lists)

keychain services 88
mail service access 240
permissions 140, 144–145, 265
print service access 338
SACLs 183, 381

Active Directory 83–84, 319

activity analysis tools 376–379

Address Book 82

addresses. *See* email addresses; IP addresses; NAT
address translation 347

administrator

accounts for 319
auditing tools 370–376
directory domain 78, 318
passwords for 329, 387
privileges of 361
administrator account 71–72, 76–81
administrator computer 39
adult websites, access control 302
Advanced Encryption Standard (AES-128) 122
AFP (Apple Filing Protocol) service
 authentication 256
 configuration 258–259
 share points 267

agents

authentication 355, 356
controllers 358
functions of 354
setup 358
Xgrid 357–359

AirPort, disabling 55

AirPort Base Station

and RADIUS 334

anonymous access, FTP 260

antivirus tools. *See* virus screening

any-user tag 351

APOP (authenticated POP) 235

appearance preferences 102–103

Apple Filing Protocol service. *See* AFP

Apple Remote Desktop. *See* ARD

Apple Software Restore. *See* ASR

AppleTalk 340

applications
access control 31, 284, 285
legacy access 289
securing 30
applications, user access to
See also specific applications
ARD (Apple Remote Desktop) 178–179
ARP (Address Resolution Protocol) spoofing 207
assistive devices 136
attributes
 ACL 267
 authentication 386
 configuration 365
audio recording devices, disabling 57
audit_class file 375
audit_control file 375
audit_event file 375
audit_user file 375
audit_warn file 375
auditing tools 370–376
auditreduce tool 373–374
audit tool 372–373
authenticated POP. *See* APOP 233
authentication
 Active Directory 83
 AFP 256
 attributes 386
 vs. authorization 26
 cached 382
 credential-based 381
 definition 380
 Directory Access 82–83
 directory services 318
 EAP 196, 334
 file services 258–259
 FTP 256
 iCal service 223
 IMAP 237
 Kerberos 192, 196, 235, 237, 238, 339, 385
 methods 326, 382
 NFS 256
 options 356, 358
 passwords 277, 278, 356, 359
 POP 235
 QTSS 348, 349, 351
 Server Admin 167
 SMB/CIFS-related 256
 SMTP 242, 243
 SSH 187–189
 strengthening methods 84–87
 system preferences 94
 user 380, 385–387, 388
VPN 192
WebDAV 275
Workgroup Manager 318–319
See also keychain services; passwords; RADIUS
authentication authority attributes 386
authorization 26–34, 79, 380
 See also authentication
authorization rights 366–367
AuthScheme keyword 351
automatic actions, disabling 105
Automatic Unicast 348

B

backups 161–162
BannerSample file, modifying 68
bayesian filters 246
Berkeley Software Distribution. *See* BSD
BIND (Berkeley Internet Name Domain) 202, 203, 206
binding 330
blacklisted servers 241, 244
blogs 280–281
blog service 280
Bluetooth preferences 55, 103–104, 117
Bonjour browsing service 210
boot image, definition 311
broadcasting, MP3 348
BSD (Berkeley Software Distribution) 25, 377
bundle IDs 284
By 139

C

CA. *See* certificate authority
cached authentication 382
cache poisoning
 DNS 205
cameras 58, 232
CDs 40
CDs, preferences 105
CDSA (Common Data Security Architecture) 25
CERT (Computer Emergency Response Team) 25
Certificate 167, 170
Certificate Authority (CA)
 requesting certificates from 169
certificate authority (CA)
 See also certificates
 overview 165
 requesting certificates from 235
Certificate Manager 167
certificates 163–175
 FileVault 153
 iChat server 226
 IPSec 192
 mail service 234–235
 management of 36–37
 Open Directory 327
 overview 163–167
 POP 236
 private keys 164

public keys 164, 368–369
requesting 170, 235
self-signed 165, 169
and Server Admin 167–168
SSL 224, 228, 277
web service 278
Certificate Signing Request. *See* CSR 233
CGI (Common Gateway Interface) scripts
enabling 273
chat service 225–229
CIFS (Common Internet File System). *See* SMB/CIFS
ClamAV 245, 249
clients
access control 348, 349
authentication 356
earlier operating systems 192
group accounts 321–322
groups 352
and SSL 234
See also client computers; users
codesign command 369–370
collaboration services
group accounts 321–322
See also mail service; specific file services
command 349
command-line interface
access warnings 69
erasing files 159–160
options 349, 350
security 256
startup security setup 64
command-line tools
erasing disks 44
log viewing 278
sudo 209
Common Criteria Tools 370
Common Data Security Architecture. *See* CDSA
Common Security Service Manager. *See* CSSM
Common UNIX Printing System. *See* CUPS
Computer Emergency Response Team. *See* CERT
computer groups 322
computer name 182
computers
idle status 358
name 182
See also portable computers
computers, administrator 39
configuration
access control 338
agents 358
controller 359
DHCP 40
Firewall service 216, 217
iChat 226–227
incoming mail 237
Kerberos 326
keychain services 89–91
Mac OS X Server file changes 203
overview 233
RADIUS 334
share points 264
SSH 186–187
VPN 193, 194
See also Mailman setup
configuration files, SSH 187
Console application 377
contacts search policy 82–83, 320
controllers
and agents 358
nodes 355
setup 359
controllers, Xgrid 359–360
CRAM-MD5 authentication 237, 238
credential-based authentication 366–367, 381
credential storage 88–93
crypt passwords
definition 382
encryption 320, 386
CSR (Certificate Signing Request) 163, 169, 170
CSSM (Common Security Service Manager) 28
CUPS (Common UNIX Printing System) 337
curfews on computer use 306
Cyrus mail service 233

D

Dashboard preferences 115–116, 285, 287
databases 318
data security 59–60, 137–162
data transport encryption 224
Date & Time preferences 107–108, 182
decryption. *See* encryption
Desktop preferences 109–110
DHCP (Dynamic Host Configuration Protocol)
service 40, 200, 330
DHX authentication 382
dictionaries
rights 363–367
Dictionary, hiding profanity in 303
digest authentication 223, 349
digest authentication, WebDAV 275
digital signatures 284, 285, 368–369
directories. *See* directory services; domains, directory;
folders
Directory Access 82–83, 320
directory domain administrator 78, 318
directory services
Active Directory 83–84, 319
directory domains 81–84
Open Directory 83
organization of 318
overview 324

- See also* domains, directory; Open Directory
- directory services, Open Directory 333
- discovery, service 82
- disk images
- encrypting 155–157
 - installing with 41
 - read/write 155
- disks
- command-line management of 44
 - erasing free space 43
 - installation preparation 43
 - partitions 41, 43
 - quotas 321
 - startup 133–134
- Disk Utility 43, 159, 160
- diskutil** tool 44
- display mirroring 111
- Displays preferences 111
- distributed computing architecture 354–360
- DNS (Domain Name System) service
- BIND 202, 203, 206
 - IP addresses 206
 - recursion 204, 207
 - securing server 205, 206
 - setup 40
- Dock preferences 111, 291–292
- documentation 21–23
- Domain Name System. *See* DNS
- domains, directory
- Active Directory 319
 - administrator for 78, 318
 - binding of 330
 - databases 318
 - LDAP 196
 - management of 318
 - overview 81–84
- See also* LDAP; Open Directory
- DoS attack (denial of service) 206, 387
- duplication of settings 319
- DVDs 40, 298–299
- DVDs, preferences 105
- Dynamic Host Configuration Protocol (DHCP) 200
- E**
- EAP (Extensible Authentication Protocol) 334
- EAP-SecurID authentication 196
- EFI (Extensible Firmware Interface) 63, 134
- email. *See* mail service
- Enabling 145
- encryption
- AFP 258
 - certificates 164
 - crypt passwords 320, 386
 - FileVault 151–157
 - mail service 235
- network configuration 197
- ports 228
- secure virtual memory 137–138
- SSH 178, 197, 257–259
- SSL 276
- VPN protocols 192
- See also* SSL
- Energy Saver preferences 112–113
- erasing data permanently 38, 158–160
- error messages. *See* troubleshooting
- Everyone permission level 141
- Exposé & Spaces preferences 115–116
- Extensible Authentication Protocol. *See* EAP
- Extensible Firmware Interface. *See* EFI
- F**
- Fast User Switching 75, 297
- fax preferences 120
- files
- access control 349
 - backup of 161–162
 - encryption 151–157, 197
 - erasing 38, 158–160
 - permissions 140–143, 146
 - qtaccess 350
 - qtgroups 350
 - qtusers 350
 - shared secret 164
 - transferring 191
- file services
- authentication 258–259
 - disabling 256
 - FTP 259–262, 268
 - NFS 262
- See also* AFP; FTP; NFS; share points
- file sharing 254–255
- file systems
- erasing data 158
 - securing 38
- File Transfer Protocol. *See* FTP
- FileVault 36–37, 53, 122, 151–155, 300
- FileVault master keychain 153
- filters
- blacklisted mail senders 241, 244
 - junk mail 245, 247
 - virus 241, 249, 251
- Finder preferences 293–294
- fingerprints, server 189
- firewalls 245, 345, 347
- See also* Firewall service
- Firewall service 213
- advanced rules setup 217
 - introduction 213
 - logs 219
 - and NAT 207

- services settings 216
settings 40
starting 214
stealth mode 218
FireWire 61, 133
FireWire Bridge Chip GUID 133
firmware, password 64
flags for files and folders 143–144
folders
 flags for 143–144
 group 321, 322
 home 81, 150–155, 267, 299
 permissions for 150
 website 273
free disk space, erasing 160, 161
Front Row 285, 288
FTP (File Transfer Protocol) service 256, 257, 259–262, 268
- G**
- GID (group ID) 320
global file permissions 146
global password policy 329
grids, computational 354
grids, computer 354
group accounts 321–322, 352
 See also groups
group filename keyword 350
group folders 321, 322
groupname keyword 350
groups
 blog service 280
 configuration 321–322
 permissions 141
guest accounts
 permissions 141, 255
- H**
- hard drive 53
hardware, protection of 52
hash, password 382
help, using 20
helper applications 289
HISEC (Highly Secure) templates 83, 319
home folders 82, 150–155, 264, 267, 299
hostconfig entries 371
host name 182
hosts. *See* servers
HTTP (Hypertext Transfer Protocol) 276, 345, 347
- I**
- iCal service 222–225
iChat service 225–229
identity certificates. *See* certificates
IETF (Internet Engineering Task Force) standard 345
images. *See* disk images; NetBoot; Network Install
IMAP (Internet Message Access Protocol)
 authentication 237
 log 250, 253
incoming mail
 security 234
 setup 237
installation
 administrator computer 39
 auditing tools 370
 with disk images 41
 disk preparation 43
 from earlier OS versions 39
 from removable media 40
 installer packages 126
 interactive 44
 network services setup 40
 overview 38–51
 server software 40
 starting up for 40, 41
installer packages 126
install image, definition 311
instant messaging 225–229
Intel-based Macintosh 63
International preferences 116
Internet-based Software Update 46
Internet Message Access Protocol. *See* IMAP
Internet Printing Protocol. *See* IPP
Internet security
 MobileMe preferences 96–98
 sharing 125
 wireless connections 56
IP addresses 118
 DHCP 200
 DNS recursion 203–204
 DNS service 206
 and firewalls 40
 groups 215
 IPv6 notation 198–199
 port forwarding 208
 QTSS 346
 and recursion 204
IPFilter service. *See* Firewall service
IP masquerading. *See* NAT
IPP (Internet Printing Protocol) 337
IPSec (IP security) 192, 193
IPv6 addressing 118, 198–199
iSight, disabling 58
ISP (Internet service provider) 192
- J**
- Jabber instant messaging project 225–229
jobs 354
junk mail screening
 connection control 241–245

filters 245, 247
log 250, 253
overview 241

K

KDC (Kerberos Key Distribution Center). *See* Kerberos
Kerberos

Active Directory 83
authentication 85–86, 192, 223, 235–238, 385
features 381, 387, 388
Open Directory 319
passwords 387
print service 339
setup 326
users 326, 388
WebDAV 275
Xgrid administration 355, 356

kernel extensions, removing 62

key-based SSH connection 187–189
Keyboard preferences 116
Keychain Access 88
keychain services 28, 30, 88–93, 153

L

L2TP/IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) 34, 192, 193

LANs (local area networks) 191, 262
layered security architecture 27

Layer Two Tunneling Protocol, Secure Internet protocol (L2TP/IPSec). *See* L2TP/IPSec

LDAP (Lightweight Directory Access Protocol)
service

advanced settings 324
configuration 83
overview 324
security 327, 331, 380
VPN 196

See also attributes; mappings; object classes;
trusted binding

LDAPv3 access 318, 324

Legacy preferences 285, 289

Lightweight Directory Access Protocol. *See* LDAP

Line Printer Remote (LPR) printing 340

local area networks (LANs) 262

local directory domains

 password types 380, 382

local installation 40

local system logging 378

local versus network home folders 264

locking folders 143

login

 access warnings 65–69

 keychain 89

 preferences 295–298

 preferences overview 295

remote 178
security measures 99–101

login scripts 296

logs

 audit 376
 configuration 377–379
 Firewall service 219
 iChat 229, 230, 232
 mail service 250, 253
 MySQL service 283
 NetBoot 314
 print service 342
 QTSS 353
 RADIUS 335
 Software Update service 317
 web service 278

LPR (Line Printer Remote) printing 340

M

Mach 25

Mac OS X

 installation considerations 39
 Open Directory passwords 381

Mac OS X Server

 agent setup 358
 authentications supported 388
 configuration file changes 203
 trusted binding 330

mail service

 certificates 234–235
 disabling 234
 group settings 321
 logs 250, 253
 security 234, 235
 virus filtering 251

mail transfer agent. *See* MTA

managed accounts 319–322

managed preferences

 Dashboard 115–116, 285, 287
 Date & Time 107–108, 182
 Desktop 109–110
 Displays 111
 Dock 111, 291–292
 Energy Saver 112–113
 Exposé & Spaces 115–116
 Finder 293–294
 Front Row 285, 288
 International 116
 Keyboard 116
 Legacy 285, 289
 Login 295–298
 Media Access 298–299
 MobileMe 96–98
 Mobility 299–301
 Mouse 116

- Network 118–119, 301–302
overview 284
Parental Controls 302, 303, 304
Print & Fax 120–122
Printing 307
Security 122
Sharing 125, 180
Software Update 46–49, 126, 308
Sound 128
Spotlight 130–132
Startup Disk 133–134
System 308–309
System Preferences 308, 309
Time Machine 161–162
Universal Access 136, 309–310
See also preferences
managed user accounts 71, 319–322
mandatory access controls 30–33
man-in-the-middle attacks 190
Media Access 298–299
message keyword 350
microphones, disabling 57
Microsoft Windows compatibilities 144
mobile accounts 82, 192, 299–301, 387
MobileMe preferences 96–98
Mobility preferences 299–301
Mouse preferences 116
movies, QuickTime cache
See also streaming media
MP3 files 348
MS-CHAPv2 authentication 195
MTA (mail transfer agent) 233
multimedia 344–353
MySQL service 282, 283
- N**
- name server. *See* DNS
naming conventions, computers 182
NAT (Network Address Translation)
 and Firewall service 207
 introduction 207
NetBoot service 41, 311–314
Network Address Translation. *See* NAT
network-based directory domains 81–84
network-based keychains 92–93
Network File System. *See* NFS
network install image 133
Network preferences 301–302
networks
 client connections 34
 preferences 302
 views troubleshooting 323
network services
 DHCP 40, 200
 DNS 40
FileVault limitations 151, 155
home folders 318
installation 40
IPv6 addressing 198–199
keychains 92
managed users 74
NTP 176
preferences 118–119, 301–302
sharing 125
sleep mode security 112
Software Update cautions 45
VPN 191–197
wireless preferences 103–104
See also IP addresses
network settings
 firewall consideration 347
Network Time Protocol. *See* NTP
newsyslog command 378
NFS (Network File System)
 file sharing 255, 262, 268
 security 256
 share points 254, 257, 268–269
nodes, controller 355
nodes, directory. *See* domains, directory
nonadministrator user accounts 71–72
NT Domain services 263–264, 340
NTP (network time protocol) 176
nvram tool 64

O

- Open Directory
 access control 349
 Active Directory 318
 binding policy 330
 configuration 83, 325–330
 definition 318
 DNS recursion 203
 and Kerberos 381
 options settings 330
 overview 324
 password type 320, 329
 and RADIUS 333
 and SACLs 183
 security policy 331
 See also domains, directory
Open Directory master
 authentication 355
 binding 330
 security policy 331
Open Directory Password Server
 access control 334
 authentication 325, 381
 password policy 387
open source modules
 Apache 271

- Jabber 226
 Kerberos 223, 275
 open source software 25–27
 option 95, DHCP 330
 Others user category 254
 outgoing mail, security 235
 Overview 152
 owner permission 141
- P**
- Parental Controls 74–75, 302, 303, 304
 partitions, disk 41–43
 Password Assistant 84–85, 100
 passwords
 administrator 329, 387
 Apache 278
 authentication 356, 359
 authentication set 84
 authentication setup 235–237
 changing 99–101
 command-line tools 64
 crypt 320, 386
 firmware 64, 133–134
 hash 382
 keychain 89
 master FileVault 151–155
 Open Directory 381, 386
 policies 329, 387
 security 384–385
 vs. single sign-on 387
 SSL passphrase 277
 Startup Disk preferences 133–134
 streaming media 348
 tokens 86
 types 380, 381, 382
 user account 351
 VPN 192
 Windows domain 386
- Password Server. *See* Open Directory Password Server
- PDFs, encrypting 157
- permissions
 access 25
 ACLs 265, 338
 administrator 361
 folders 150
 guest 255
 manipulating 143
 overview 140–146
 share points 265–267
 types 254
 user 274, 278, 320–322
 viewing 141
 WebDAV 274
- physical access, securing 53
- physical computers
 hardware security 53
- piggybacking, service 207
- PKI (public key infrastructure) 163, 164
See also certificates
- playlists
 accessing 349
 QTSS 344
- plist files 209
- Podcast Producer service 231–232
- policy database 363–367
- POP (Post Office Protocol) 236, 250, 253
- port 347
- portable computers
 FileVault 151
 keychains 92–93
 mobile accounts 82, 192, 299–301
 portable files, encrypting 155–157
 portable keychains 92
 port forwarding 208
- ports
 encryption 228
 QTSS 345–347
 and SSL 276
 VPN 193
- POSIX (Portable Operating System Interface) 141–146
- Postfix transfer agent 233
- Post Office Protocol. *See* POP
- PPTP (Point-to-Point Tunneling Protocol) 192, 194
- praudit tool 374–375
- preferences
 accounts 99–101
 appearance 102–103
 Bluetooth wireless 103–104, 117
 CDs 105, 298–299
 DVDs 105
 fax 120–122
 login 295–298
 overview 94–95
 screen saver 109–110
 speech recognition 129
 time 107–108, 182
See also managed preferences
- presets 319
- primary zone, DNS 205
- Print & Fax preferences 120–122
- print service
 access control 307, 338
 security 337
- private key 164, 165
- private key cryptography 276
- privileges, administrator 361
See also permissions
- problems. *See* troubleshooting
- profanity, hiding 303

profiling, DNS service 206

protocols

EAP 334

file services 257

HTTP 276

LDAP 196

network service 40

POP 236, 250, 253

RTP 345

RTSP 345

TCP 216

VPN 192, 193, 194, 196

See also specific protocols

proxy server settings 301–302, 346

public key certificates 189

public key certificates. *See* certificates

public key cryptography 276, 368–369

public key infrastructure. *See* PKI

`pwpolicy` command 86

Q

`qtaccess` file 350

`qtgroups` file 350

`qtpasswd` tool 349

QTSS. *See* QuickTime Streaming Server

`qtusers` file 350

Quarantine 32

queues, print

 creating 340

 logs 342

QuickTime Streaming Server (QTSS) 344–353

quotas, disk space 321

R

RADIUS (Remote Authentication Dial-In User Service)

 introduction 333

read/write disk images 155

Really Simple Syndication. *See* RSS

realms. *See* Kerberos; WebDAV; websites, accessing

recent items list 102–103

recursion, DNS 203–204, 207

relays, access control 349

Remote Apple Events 181

Remote Authentication Dial-In User Service

 (RADIUS). *See* RADIUS

Remote Login 185–186

remote servers

 login 178

 system logging 378

removable media

 FileVault limitations 151, 155

 installation from 40

 preferences 298–299

removable media, accessing 299

rights dictionary 363–365

right specifications 363–365

root permissions 63, 79–80

RSA SecurIDs 196–197

RTP (Real-Time Transport Protocol) 345

RTSP (Real-Time Streaming Protocol) 345

rules 365

S

SACLs (service access control lists) 183, 228, 259,

 261, 338, 381

sandboxing 31

`scp` tool 185

screening

 virus 251

See also filters

screen saver preferences 109–110, 122

searching

 Spotlight 273

searching preferences 130–132

Secure Empty Trash command 160

secure notes 88

Secure Shell. *See* SSH

Secure Sockets Layer. *See* SSL

Secure Transport 27

SecurID 196–197

Securing 210

security

 ACLS 338

 authentication 223

 best practices 254

 certificates 327

 DNS 205, 206

 firewall 245

 firewalls 345, 347

 Firewall service 40

 IPSec 192, 193

 LDAP 327, 331, 380

 NetBoot service 312

 network 256

 overview 234

 passwords 235–237, 348, 351

 print service 339

 QTSS 345, 347

 server policy settings 331

 service level 183

 SSL 226–228, 234–239, 276, 327

 tools 222, 224

 VPN 192

 websites 276, 278

 wiki 229

See also access; authentication; permissions

security architecture overview 25–28

security-mode environment variable 64

security-password environment variable 64

Security preferences 122

Security preferences<\$endrange 126
self-signed certificates 165, 169, 235
Server Admin
 access control 190, 240, 255, 338
 as administration tool 271
 authentication 167, 195
 certificates 169
 opening 167
 overview 163, 167
 server status 203
Server Message Block/Common Internet File System.
 See SMB/CIFS
server mining 205
servers
 binding to 330
 blacklisted 241, 244
 naming 182
 proxy 301–302, 346
 securing DNS 205, 206
 security policy 331
 SMTP 242
 startup 40, 41
 See also Apache web server; remote servers;
 websites
server side includes. *See* SSI
service access control lists. *See* SACLs
services, security 183
setup procedures. *See* configuration; installation
SFTP (Secure File Transfer Protocol) 191, 257–259
sftp tool 185, 268
SHA-1 digest 50
shadow passwords
 definition 382
 features 386
shared files. *See* file sharing
shared resources
 printers 120
 user accounts 72
shared secret files 192
share points
 configuration 264–268
 home folders 264
 NFS 254, 262
 setup 264
Sharing preferences 125, 180
Simple Finder 293
Simple Network Management Protocol (SNMP) 177
single sign-on (SSO) authentication 86, 355, 356,
 387
single-user mode 63
sleep mode, securing 112–113, 122
sleep settings, securing 292
smart cards 36–37, 86, 91, 320, 389
SMB/CIFS (Server Message Block/Common Internet
 File System) protocol
 authentication 256
enabling 263–264
printing 340
security overview 258
share points 267
SMTP (Simple Mail Transfer Protocol) 242–245, 250,
 253
SNMP (Simple Network Management Protocol) 177
Snow 163
Software Update service 45, 46–49
 clients 316
 configuration 308
 disabling 315
 overview 316
 preferences 126
 settings 316
 starting 315, 333
Sound preferences 128
sources 259
sparse images 155
speech recognition preferences 129
spoofing
 ARP 207
Spotlight preferences 130–132
Spotlight searching 273
srm command 159–160
SSH (secure shell host) 178, 185–191, 197, 259
sshd daemon 185
ssh tool 186
SSI (server side includes) 273
SSL 237
SSL (Secure Sockets Layer)
 certificates 164–167, 227, 228
 iCal service 224
 iChat service 226
 mail service 234–240
 Open Directory 327–329
 overview 27
 web service 276
standard user accounts 71
startup, securing 63
Startup Disk preferences 133–134
stealth mode, Firewall service 218
streaming media 344–353
sudo tool 79–82, 209, 361
su tool 80
synchronization 96–98
 mobile account data 299
 time 176
syslogd configuration file 377
system administrator (root) account 79–82
System Preferences 308–309
 See also managed preferences

T

target disk mode 134

tasks 354
TCP (Transmission Control Protocol) 213, 216, 345
The 30
third-party applications 115
ticket-based authentication 83
time limits on computer use 306
Time Machine 30–31, 134, 161
time settings 107–108
time synchronization 176, 177
time zone settings 182
TLS (Transport Layer Security) protocol
tokens, digital 86
Transmission Control Protocol (TCP) 213
Transport Layer Security protocol. *See* TLS
transport services 27
troubleshooting
 network views 323
 QTSS 353
trusted binding, policies 330

U

UDP (User Datagram Protocol) 345, 347
UIDs (user IDs) 73, 284
Universal Access
 overview 309
 preferences 309–310
Universal Access preferences 136
UNIX 289
UNIX and security 25
updating
 software 126, 308
updating software 45–49
USB storage devices, disabling 60
user accounts
 administrator 319
 group 321–322, 352
 in directory domains 319
 mobile 299–301
 overview 71–81
 passwords 351
 security 71
 settings 75
 See also users
user filename keyword 350
user ID. *See* UID
username keyword 350
users
 access control 30–33, 71–75, 190, 274, 348, 349,
 351
 auditing 376
 authentication 324–325, 326, 380, 385–387, 388
 automatic actions control 105
 and blog service 280
 categories 254
 certificates 165

Fast User Switching 297
home folders 82, 150–153, 267, 299
identities 284
keychain management 91
mobile 82, 192
passwords 320
permissions 141, 274, 278, 320–322
preferences control 115
root 63
unregistered 255
wireless access 333
See also clients; computer lists; preferences; user accounts; Workgroup Manager

V

validation, system integrity 368–370
valid-user tag 351
video recording devices, disabling 58
view settings 323
virtual memory 137–138
Virtual Private Network. *See* VPN
virus screening 241–249, 250, 251, 253
visudo tool 361
volumes
 erasing 44
 erasing data 158
 securing 38
 startup 41
VPN (Virtual Private Network)
 authentication 192
 clients 34
 introduction 191–197
 L2TP settings 34, 193
 and LDAP 196
 PPTP settings 194
 security 192

W

WAN (wide area network) 191
Web 271
WebDAV (Web-Based Distributed Authoring and Versioning)
 authentication 275
 configuration 279
 enabling 273
 permissions 274
 realm definitions 274
 starting 273
weblog service 280–281
web modules 273
web service 272–278
websites
 access control 274
 accessing 302–304
 folders 274

security 229, 276
wide area network. *See WAN*
widgets in Dashboard 285, 287
wikis 229
Windows domain
 passwords 386
Windows services 263–264, 340
wireless preferences 103–104
workflows 231
Workgroup Manager
 access control 32
 accounts 319–322
 ACL permissions 240
 authentication 349
 directory domains 318
group account management 321–322
overview 318–319
 See also managed preferences
workgroup preferences
 See Workgroup Manager
World permission level 254

X

Xgrid 354–360

Z

zones, DNS
 security 205
zone transfer, DNS 203