Report Number: I331-003R-2005

Apple Mac OS® X Server v10.3.x "Panther"

Security Configuration Guide

Systems and Network Attack Center (SNAC)

National Security Agency
9800 Savage Rd.
Ft. Meade, MD 20755-6704

Warnings

- Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Apple Mac OS X v. 10.3.x "Panther" and should not be applied to any other Mac OS versions or operating systems.
- This document is current as of July 8, 2005. See http://www.apple.com for the latest changes or modifications to the Mac OS X v10.3.x "Panther" operating system.

Trademark Information

Table of Contents

Introduction

The purpose of this guide is to provide an overview of Mac OS X Server v10.3 operating system security and recommendations for configuring its security features. This guide tries to provide recommendations for many different roles a Mac OS X Server system can assume in a network.

This guide is intended for administrators of Apple Mac OS X Server v10.3.x systems and it is assumed that anyone using this guidance will be an experienced Mac OS X user, will be familiar with the Mac OS X user interface, and will have at least some experience using a command-line interface (e.g. the Terminal program). In addition, anyone using this guidance should have experience in administering a network, be familiar with basic networking concepts, and be familiar with Apple's system administration guidance (listed in the References chapter).

Some instructions within this guidance are complex, and deviation could result in serious adverse effects on the system and its security. Modification of these instructions should only be performed by experienced Mac OS X administrators, and followed by thorough testing.

Getting the Most from this Guide

The following list contains suggestions for successfully using the Apple Mac OS X Server Security Configuration Guide:

- Read the guide in its entirety. Subsequent sections may build on information and recommendations discussed in prior sections.
- This guidance should always be tested in a non-operational environment before deployment. This non-operational environment should simulate the architecture where the system will be deployed as much as possible.
- This guidance is intended primarily for Mac OS X Server systems. Before applying this guidance to a system, an administrator should determine what function that particular system will perform, and apply the applicable sections of this guidance.

Any deviations from this guidance should be evaluated to determine what security risk it may introduce, and measures should be taken to monitor or mitigate those risks.

Scope of Guidance

Apple's Mac OS X operating system is very versatile and can be used not only as a client workstation, but also to manage and serve entire networks of machines and users. Apple offers two versions of the operating system: **Mac OS X** and **Mac OS X Server**. The two products offer many of the same administration and configuration features. The server version provides additional tools designed to assist the administrator in managing networks of computers and users, to include other environments such as Windows and other UNIX-based systems. The default configuration for Mac OS X Server is not as "locked-down" from a security standpoint as Mac OS X. This is by design, since a server being used to administer an entire network will typically need more services available.

The goal of this guidance is to provide instruction on securing Mac OS X Server systems, including secure configuration of a system running Mac OS X Server 10.3.x; the management of network vice local user accounts; managing Mac OS X 10.3.x clients using Mac OS X Server 10.3.x; the configuration of specific server functions, such as mail or web services; and using the built-in IP filtering features.

This guidance is designed to give instruction on securing a Mac OS X Server 10.3.x system, and on securely managing Mac OS X servers and clients in a networked environment. It does not provide instruction on securing a Mac OS X client machine. For assistance in securing Mac OS X 10.3.x clients, please see the "Apple Mac OS X v10.3.x Panther Security Configuration Guide." It also does not provide complete guidance on installation of a Server and the various services that may be run on that machine. For information on correctly installing and configuring server and server functions, consult the Apple system administration guidance, listed in the References chapter.

This guidance cannot cover all possible network architectures where Mac OS X Server might be used. The instructions here are designed to assist the administrator in designing a secure network architecture using Mac OS X Server, in making sure systems used in the designed network are configured securely, and in determining the best ways to securely manage OS X systems in a networked environment. Good network security and design must be used for this guidance to be effective, and it is expected that anyone using this guidance will be familiar with general computer and network security principles.

Finally, it is assumed that anyone using this guidance is familiar with UNIX security basics, such as setting file permissions, setting file paths, and use of the setuid bit. These security basics are well documented; therefore, this guide will not address them.

Guidance in this document is intended for a system running Mac OS X Server 10.3.x and may not be applicable to other versions.

1. Introduction to Mac OS X Server Security

Mac OS X Server combines the GUI-based, user-friendly features of the Macintosh operating system with the underlying foundation of a BSD Unix system. This chapter provides an overview of features in Mac OS X Server that can be used to enhance security in a networked environment.

Mac OS X Server 10.3.x has the same basic architecture as Mac OS X, but adds a number of tools to facilitate administration of multiple machines, services, and users. Mac OS X Server also includes additional network services. For an overview of the security features common to both systems, see the NSA "Apple Mac OS X v10.3.x Panther Security Configuration Guide." For a more complete discussion of features in Mac OS X Server, please see Apple's "Getting Started with Mac OS X Server 10.3."

1.1 Centralized User Account Management

Mac OS X Server provides a way for administrators to centrally manage user accounts and other user information. Accounts no longer have to be maintained on individual clients, greatly simplifying account management. Storing user account information on a physically secure server dedicated to that purpose also brings security benefits.

Open Directory is the name of the directory service through which a server and its clients handle this user account information. Open Directory can perform user authentication using several different methods, including protocols native to the Windows environment and existing NetInfo directories. However, it is based on Open Directory LDAP, which provides LDAPv3 directories. The Open Directory framework can also provide cross-platform communication with Active Directory servers, BSD configuration files, Sun Microsystems NIS files, and other LDAPv3 servers. Secure Sockets Layer (SSL) support is available for LDAPv3 communications. Additionally, Open Directory can enforce password policies, such as setting a password length and making passwords expire periodically.

Open Directory can be configured to perform user authentication using Kerberos v5. This can be accomplished using pre-existing Kerberos environments, or Mac OS X Server can be used to establish a Key Distribution Center (KDC). Using Kerberos for user authentication gives the user single sign-on capability when accessing services that support Kerberos authentication.

1.2 Centralized Client Settings Management

Although system preferences on Mac OS X client systems can be set individually by an administrator, these settings should be centrally managed by Mac OS X Server whenever possible. Centralizing client system preferences enhances security by enforcing the most secure settings on all systems. For example, users of managed client systems can be prevented from using recordable media, restricted to using only certain printers, and even denied access to making any changes using the System Preferences program. Lists of client systems can be created to tailor the settings for particular groups of systems as required.

1.3 Network Services

Mac OS X Server includes software to provide network services including:

- E-mail
- Web
- Print
- DNS
- Firewall
- VPN

Mac OS X Servers can also be used as Application servers. In general, the services included with Mac OS X Server are based on recent releases of open-source projects and provide the most recent security enhancements available. With proper configuration, these services allow a network to attain a very high security stature.

2. Network Architecture

Careful planning that incorporates security concerns must precede deployment of Mac OS X Server in any network architecture. Apple's Mac OS X Server Administrative guides at http://www.apple.com/server/documentation provide worksheets to assist in this process. Providing adequate isolation of the site network from the outside world and properly separating functions for the computers within the site network are basic security goals in designing a network.

2.1 Network Isolation

The site's connection to external networks such as the Internet must be properly protected. In general, this involves using a firewall to filter network traffic. The firewall should prevent unwanted access to your network and its resources from computers on the external network. For example, it's common to set up file sharing services such as AFP or SMB on a local network. Such services should not be available to external users, and certainly not to external networks or the Internet at large. A properly configured firewall can prevent external users from accessing the file server.

Other measures such as intrusion detection systems, proxy servers, and host-based firewalls can further bolster network defenses. Design of the site's external connections is out of the scope of this guide. Cheswick and Bellovin's "Firewalls and Internet Security – Repelling the Wily Hacker" provides an introduction to many of the issues involved. The NSA "Router Security Configuration Guide" provides information on configuring some network boundary devices and using them as firewalls.

2.2 Function Separation

Any computer system on a local area network can be classified into one of three main categories: directory servers, other servers, and client systems. Any system on the network should fall into exactly one of these categories, and never serve as one of the others.

Directory servers are distinguished from other types of servers because they are used to manage user and client system settings and contain user authentication data. Planning the structure of the hierarchy of directory servers, including replicas and backups, is especially important to ensure availability to all users. The "Open Directory Planning" chapter in Apple's "Mac OS X Server Open Directory Administration Guide" provides a detailed explanation of this planning process. Directory servers should be kept in a physically secure location to which non-administrative personnel do not have access, and network access to these servers

should be as restrictive as possible. Only administrative users should be able to log directly onto a directory server. Examples of directory services are: Apple's LDAP-based Open Directory Server included with Mac OS X Server, Microsoft's Active Directory, and Sun's NIS/NIS+.

A typical network also includes servers for network services such as e-mail, file sharing, logging, and web. To the maximum extent possible, each network service should be hosted on a separate server. Physical access should be restricted to administrative personnel wherever possible, network access should be restricted to only that which is operationally necessary, and only administrators should be able to log directly into a server.

Client systems provide user access to the network but do not provide any services to the rest of the network. Security-relevant settings on the client should be enforced to the maximum extent possible. Configuration guides from NSA exist for Mac OS X, Solaris, and Microsoft Windows. The Center for Internet Security publishes configuration guidance for systems running Linux, FreeBSD, and HP-UX.

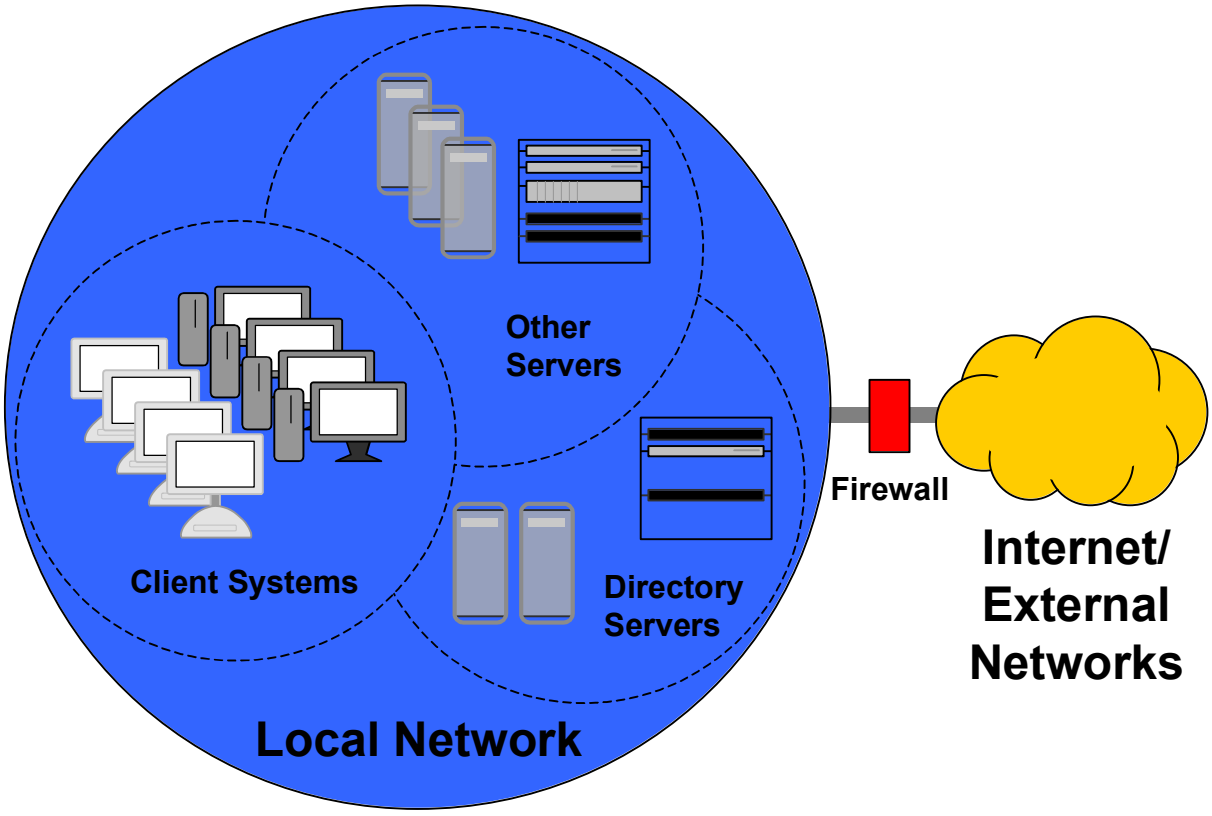

Figure 1: Basic Network Design

3. Basic Installation and Configuration

Although secure configuration of an existing Mac OS X Server installation is possible, securely configuring a fresh installation is much simpler. This may not always be practical, but it is the recommended way to configure Mac OS X Server. If this guide is being used to configure a previously installed server, the Installation section of this chapter, which discusses installing a new machine from CD, will not apply for the most part. The administrator should still read this section, however, and modify the previous installation to make it match the recommended installation as much as possible. This may entail deleting installed packages, disabling services, changing an administrative account name, installing updates, and fixing disk permissions. This guide does not provide instructions on making these types of modifications to a previously installed system. Also, administrators should be aware that applying these recommendations to an existing system might cause the system to operate incorrectly.

The section addressing updating the operating system and installing security patches to the system should be performed on all servers.

The section of this chapter on additional configuration of a Mac OS X server should be applicable to all OS X servers. Caution should still be used if performing this configuration on an existing system, as making these types of changes to an operational system could cause conflicts with the current configuration.

Systems should remain isolated from the operational network until they are completely and securely configured whenever possible; use of an isolated test network is recommended for installation and configuration.

3.1 Before Installation

If the Open Firmware password was previously enabled, it should be disabled before beginning installation. To do this:

1. Hold down ⌘-option-O-F while restarting the system to enter Open Firmware mode.
2. Enter the Open Firmware password when prompted.
3. At the Open Firmware prompt (“>”) enter:

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

The installation process will destroy all information on the hard drive. If any information on the system should be retained, it should be backed up before beginning this installation. When backing up and restoring any information, the following guidelines should be used:

- Only user files and data should be saved and later restored; restoring system settings or previous accounts may change the system configuration specified in this guidance.
- Applications should be re-loaded from the original media, not restored from a backup.

3.2 Installation

To begin a system installation, boot from a Mac OS X Server installation disk inserted in the CD/DVD drive by holding down the "C" key while rebooting the system. All data on the target drive will be lost during the installation process.

The following instructions will cause all information on the target drive to be lost. Backup any data on the system that should be retained.

The following instructions should be performed during the installation process. Only options that have security implications are covered here, and they appear in the order in which they appear during the installation process. For any option not discussed below, the administrator may choose the settings according to operational need.

1. Before starting the installation screens, the disk should be formatted and the startup disk should be chosen. This is done using the Disk Utility program, which can be started from the Installer menu.
    - It is recommended that the entire drive be re-formatted rather than just the partition where Server is to be installed. After the entire drive is formatted, partitions can be created as required. This is done to ensure Mac OS 9 drivers are not installed on the drive. If the entire drive is not re-formatted as described here, Mac OS 9 drivers may be installed on the machine, and should be removed.
    - Choose the partition or drive to be formatted.
    - If there is an option to install the Mac OS 9 Disk Driver in the window, make sure this option is not selected (click to uncheck box.)

- Erase and format the drive using either the Mac OS Extended (Journaled) or the Mac OS Extended (Case-sensitive/Journaled) option.
- Quit Disk Utility when finished.

2. When the installation program asks for the destination volume, select the drive or partition where Server is to be installed. If this drive or partition was formatted in step 1 above, continue the installation. If it was not, click the "Options" button and select "Erase and Install," setting the file type to Mac OS Extended (Journaled).
3. At the “Install” screen, click on the customize button.
4. Deselect any options not needed on this server. Any unneeded languages should not be installed. Also, only drivers for the printers that will be used by the system should be installed. Open the Printer Drivers option, and deselect any drivers that will not be needed. (Printer drivers can always be installed at a later date if a new printer is added.)
5. Continue the installation.
6. The disk check should not be skipped.

After the system finishes copying files and loading the operating system, installation screens will continue. The following specific settings or recommendations should be used:

7. When entering the administrative account information:
   - For both the Full Name and the Short Name, use names other than "administrator," "admin," or some form of the word administrator. The name alone should not identify the account as an administrative account.
   - Use a strong password. Passwords can be up to 255 characters long and contain uppercase letters, lowercase letters, numbers, and special characters. Choose a password that consists of at least 12 characters, that would not be found in a dictionary, and that contains mixed case, numbers, and special characters.
8. When entering the machine name, the name should not indicate the purpose of the machine. The word “server” should not be used as the name or part of the name.
9. When selecting the Network Interfaces to be used, select only those that will be used and deselect all others. For example, if the network interface for the server will be Built-in Ethernet only, click to deselect Built-in FireWire. AppleTalk should not be used.
10. On the TCP/IP Connection screen, “manually” should be selected for the Configure setting. Use of DHCP or BootP is not recommended.

11. For now, the “Set directory usage” setting on the Directory Usage screen should be set to Standalone Server to simplify the installation process. The type of directory usage depends on the role of the server being installed. The directory usage will be fully set up later in the guidance.

12. On the Services screen, do not enable any services yet. The services that should be enabled depend on the role of the server being installed. Each service should be configured carefully before activation.

13. On the Network Time screen, a network timeserver should be specified if a local timeserver is available. Either do not select to use a network timeserver, or select the “Use a network timeserver” box, and type the name or address of the local timeserver in the NTP Server box. Some authentication services, including Kerberos, require that time be synchronized across all machines, which necessitates synchronization with a timeserver. If necessary, one timeserver on the local network may synchronize with a trusted Internet timeserver, but it is the only server that should do so. Direct use of an Internet timeserver is not recommended for other servers.

    If NTP is to be used on a network without Internet access, the system providing the NTP service will need to either have another time source connected, such as a GPS unit, or will need to be set up to use an undisciplined local clock. See http://www.ntp.org for full documentation and instructions on configuring an NTP server on an isolated network.

3.3 Update the System

System updates should be installed immediately after the operating system installation. At the time of the writing of this guide, the most recent system update is "Mac OS X Server Update Combined 10.3.8.” The guidance in this document has been confirmed under these updates. If newer security updates are available, they should be installed.

After Mac OS X Server v10.2.8, all security updates contain only fixes for security issues. It is possible to review the contents of each security update before installing it. To see the contents of a security update, go to Apple’s Security Support Page (http://www.apple.com/support/security) and click on the “Security Updates page” link.

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

Updates can be downloaded from http://www.apple.com/support/downloads using a machine designated specifically for downloading and verifying updates, and should be copied to a disk for installation. The download should be done separately so that file integrity can be verified before the updates are installed.

Administrators should note that updates provided through the Software Update utility might sometimes appear earlier than the standalone updates.

Note the SHA-1 digest for each update file downloaded, which should be posted on-line with the download.

Once the software updates have been downloaded they should be checked for viruses and written to a CD. Use the SHA-1 digest to verify the integrity of each update using the following command:

```
/usr/bin/openssl sha1 <full path filename>
```

The `<full path filename>` is the full path filename of the update for which the SHA-1 digest is being checked. Repeat this for each update.

The SHA-1 digest for each update should match the digest given on Apple's web site for that update. If it does not, the file was corrupted in some way and a new copy should be obtained.

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

3.4 Fix Disk Permissions

Permissions on files can sometimes become set incorrectly, especially during a software installation. Incorrect permissions can cause the system to operate incorrectly and even introduce security vulnerabilities. Fixing these permissions is recommended after performing any software installation on Mac OS X Server. To fix permissions, start the Disk Utility application found in `/Applications/Utilities`, select the partition or drive where Server was installed, and click on "Fix permissions."

The procedure for repairing disk permissions should be performed after every software installation, including the operating system, updates, and applications.

3.5 Configuring System Preferences

Basic system configuration follows the installation of the operating system and its updates. All system configuration guidance given in this chapter should be performed from an administrator's account.

The **System Preferences** program provides a graphical interface for controlling many of the system security features. To start the System Preferences program, select **System Preferences...** from the Apple menu at the top left corner of the screen, or click on the System Preferences icon in the dock. The System Preferences program will start in a "Show All" view, displaying icons for configurable system features.

The following sections review options in the System Preferences application with security implications and indicate recommended settings.

3.5.1 Desktop and Screen Saver

The **Desktop and Screen Saver** option in System Preferences should be used to automatically start the screen saver when the computer has been idle for a specified amount of time, such as 10 minutes. When used in conjunction with requiring a password to wake the machine from sleep or the screen saver this will help prevent an unattended system from being used by unauthorized users.

3.5.2 Security Settings

The **Security** option in System Preferences controls the FileVault user home directory encryption feature and allows the administrator to require the password to wake from sleep or the screen saver.

The FileVault feature for encrypting home folders is recommended for systems that store home directories and whose physical security cannot always be guaranteed, such as portables like the iBook and PowerBook. FileVault cannot be enabled on home directories stored on a file server as would be typical in a network environment. See the NSA "Mac OS X 10.3.x Panther Security Configuration Guide" for information on configuring FileVault. Information on FileVault is also available in Mac Help, from the Finder's Help menu in the topics "About FileVault," "Encrypting your home folder," and "Turning off FileVault."

The setting "**Require password to wake this computer from sleep or screen saver**" affects only the account currently logged in, but the administrator account is the only account that should be locally logging into the server. Place a check in the box for **Require password to wake this computer from sleep or screen saver**.

3.5.3 Bluetooth

The **Bluetooth** panel in the System Preferences program facilitates configuration of that wireless communications standard, used by devices such as wireless keyboards, wireless mice, and cellular phones. This panel will not appear on machines not equipped with Bluetooth hardware support. If this icon does not appear in the System Preferences panel of the machine being configured, skip to the next section.

Bluetooth should not be used, and should be disabled in the Bluetooth panel within System Preferences. Though System Preferences may be used to disable Bluetooth, there are a few notes about the management of Bluetooth in Mac OS X:

- This panel only disables Bluetooth for the currently logged in user.
- Bluetooth, IR ports, CD writers, and any other hardware capability that could be dangerous in a secure environment should be physically disabled if possible; however, disabling or modifying the hardware will likely void the warranty on the machine if it is not performed by an Apple Certified Technician. For information on becoming an Apple Certified Technician, send a request for information to the Apple Federal e-mail address: AppleFederal@apple.com.

Additional steps for disabling Bluetooth are presented in a later section of this chapter.

3.5.4 CDs & DVDs

The server should not perform an automatic action when a CD or a DVD is inserted. As with Bluetooth, setting this option using the System Preferences program applies to the current user on the server only (which should be the administrator). Further instruction on controlling media access by users on client systems is given in later sections of this guidance.

To prevent automatic actions when a disk is inserted (for the currently logged in account,) select “Ignore” for all selections in the CDs & DVDs panel of System Preferences.

3.5.5 Energy Saver

The Energy Saver panel allows an administrator to configure the computer to sleep after a period of inactivity. Use of these features can lead to a denial of service on a server system. These settings should be configured as follows:

1. Open System Preferences and click on the **Energy Saver** icon.
2. Set the **Put the computer to sleep when it is inactive for:** slider to **Never**.
3. Click on the **Options** button in the Energy Saver panel.

4. Uncheck the checkbox in front of the **Wake when the modem detects a ring** option to disable it.
5. Uncheck the checkbox in front of the **Wake for Ethernet network administrator access** option to disable it.
6. Uncheck the checkbox in front of the **Allow power button to sleep the computer** option to disable it.
7. Uncheck the checkbox in front of the **Restart automatically if the computer "freezes"** option to disable it. Behavior that causes the system to freeze should be investigated because it may be malicious.

3.5.6 Sound

The microphone setting in the **Sound** panel may present security risks. This is especially important because an internal microphone is standard on many Macintosh computers. The number and type of devices that appear for sound input will vary depending on the hardware configuration of the machine.

To secure the input settings for the machine:

- Set the input volume for each device in the Input settings section of the System Preferences sound panel to the lowest possible setting. Some devices, such as "Digital In," may not have a volume control.
- Make sure the device selected for sound input is NOT the internal microphone, assuming there is another device listed in the Input settings.
- Make sure no external audio input devices are attached, especially to the device that was chosen in the input settings. For example, if "Line In" was selected as the input device, make sure a microphone is not attached to the Line In of the machine.
- If there is a Line In jack on the machine, a "dummy plug" should be used to block that jack.
- If there is an internal microphone in the machine, it should be physically disabled. As explained in the section on Bluetooth above, disabling or modifying the hardware will likely void the warranty on the machine if not performed by an Apple Certified Technician. For information on becoming an Apple Certified Technician, send a request for information to the Apple Federal e-mail address: AppleFederal@apple.com

Additional instructions for disabling the microphone appear in a later section of this chapter.

3.5.7 Network

AirPort and Bluetooth wireless connectivity options should be turned off. They will only be present in the panel if supporting hardware is installed on the system. To configure the network settings:

1. Open the **Network** panel in System Preferences.
2. Pull down the **Show** menu and select **Network Status**.
3. For each active interface in the status list, double-click the interface entry to edit it, click on "Configure IPv6…," and make sure the selection for "Configure IPv6:" is set to "Off."
4. Pull down the **Show** menu and select **Network Port Configurations**.
5. If present, make sure the AirPort and Bluetooth boxes in the **Port Configurations** list are unchecked. Also, uncheck the Internal Modem box if it is present and the modem is not operationally required.
6. Pull down the **Location** menu and repeat step 3 for any additional locations in the menu.
7. Click the **Apply Now** button.

Anytime a new location is added to the configuration, AirPort, Bluetooth, and Internal Modem should be disabled as described here.

Any wireless capability such as AirPort and Bluetooth should be physically disabled in secure environments. Disabling or modifying the hardware will likely void the warranty on the machine if not performed by an Apple Certified Technician.

Instructions for removing Airport and Bluetooth software are presented in a later section of this chapter.

3.5.8 Sharing

The default installation has the services in the Sharing panel switched off except Remote Login. All services should be disabled unless required because they may provide a means for an unauthorized user to access the machine remotely.

The services available in this panel are:

- **Remote Login**: This service allows users to access the machine remotely using SSH and should be deselected if not required. If a remote login capability is required, using SSH is still preferable to telnet.
- **Apple Remote Desktop**: This allows the machine to be managed via the **Remote Desktop** program. Managing a server with remote desktop is not recommended.

- **Remote Apple Events**: This service enables the machine to respond to Apple events from other computers, which may present security risks. Configuring this capability is out of scope for this guide and it should remain disabled.

3.5.9 Accounts

The **Accounts** option in System Preferences allows administrators to create and configure local user accounts. On a Mac OS X Server system, the only accounts configured here should be for the system administrators. To edit Accounts settings:

1. Open System Preferences and click on the **Accounts** icon.
2. Click on the **Login Options** item.
3. Select **Name and password** as the setting for **Display Login Window as:**. This causes the login window to require both a user name and a password to be entered. If the **List of users** option is set, the system will provide a list of all valid user accounts. Such information should never be automatically displayed.
4. Uncheck the box for **Automatically log in as:** if it is checked. If this box is checked, no login is required for the machine; the user selected in this option is always automatically logged in. A user should always be required to authenticate to gain access to the system.
5. Place a check in the **Hide the Sleep, Restart, and Shut Down buttons** checkbox to prevent a user from attempting to reboot the machine into single user mode without first logging into a valid account. This will not prevent a user from pulling the power cable to abruptly shut down the computer, unless the power cable is inaccessible to the user. Further protection for this problem will be discussed later in this chapter.
6. Uncheck the box for **Enable fast user switching** to disable it.

3.5.10 Date and Time

Some system services, such as the Kerberos authentication system and some e-mail servers, require that the system keep correct time. To configure date and time:

1. Open System Preferences and click on the **Date & Time** icon.
2. Click on the **Date & Time** button at the top of the panel.
3. Set the date and time for the machine.
4. If a local, trusted NTP server is available, enter it into the text field and check the box for **Set Date & Time automatically**. Otherwise, uncheck the box.
5. Click the **Time Zone** button at the top of the panel and select the appropriate time zone.

3.5.11 Software Update

Software updates should not be performed automatically. All update downloads should be conducted on a machine other than the one being configured. The Software Update feature should be configured as follows:

1. Open System Preferences and click on the **Software Update** icon.
2. Uncheck the box in front of **Check for updates**.

3.6 Configuring Directory Access

The Directory Access program in `/Applications/Utilities` can be used to control how and where the system searches for authentication information, and what network service discovery protocols to use. To configure recommended settings:

1. Open the Directory Access Program.
2. Unlock the window if necessary.
3. Uncheck all unnecessary boxes. The AppleTalk, SLP, SMB, and Rendezvous protocols allow automatic network service discovery, which is not recommended. Providers of network services should always be manually specified. NetInfo and BSD Flat File/NIS are not recommended because they are legacy directory service protocols; LDAP is preferred. Active Directory should only used if required.
4. If LDAPv3 is required, select the item and click Configure. A dialog box will appear.
    a. If necessary, expand the window by clicking “Show Options.”
    b. Uncheck the box for “Use DHCP-supplied LDAP Server.”
    c. Click New to create a new entry describing the LDAP server.
    d. In the “Server Name of IP Address” column, enter the IP address of the server.
    e. Check the box for SSL to enable encrypted network communications. (Information on installing SSL certificates is provided in the section “Creating an SSL Certificate for LDAP Services.”)
    f. When the entry is complete, click OK to close the dialog box and return to the main window.
5. If Active Directory is required, select the item and click Configure. A dialog box will appear.
    a. If necessary, expand the window by clicking “Show Advanced Options.”

b. Uncheck the box for “Cache last user logon for offline operation” unless it is required.

c. Uncheck the box for “Authenticate in multiple domains” unless it is required.

d. When the entry is complete, click OK to close the dialog box and return to the main window.

6. Click the Authentication tab.

   a. In the **Search:** pop-up menu, select **Custom path**.

   b. Click the **Add…** button to bring up a dialog box.

   c. Add only the directories necessary.

7. Click Apply.

3.7 Setting the Global umask

The **umask** setting determines the permissions of new files and folders created by a local user. The default umask setting, 022, removes group and world write permissions. With a umask setting of 027, files and folders created by a user will not be readable by every other user on the system but will still be readable by members of his assigned group. The owner of the file or folder can still make it accessible to others by changing the permissions in the Finder’s Get Info window or by using the chmod command. The NSUmask setting for all local users can be set to octal 027 (decimal equivalent 23) by issuing the following command in a Terminal window:

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

Note that the path above refers to the domain .GlobalPreferences, not to the file .GlobalPreferences.plist, which might accidentally be filled in while using the shell autocomplete feature.

This command will affect the permissions on files and folders created by programs that respect the Mac OS X NSUmask settings. Programs should follow the value set for NSUmask, but there is no guarantee that they will. Also, users can override their own NSUmask setting at any time. The changes to the umask settings take effect at next login.

3.8 Securing Initial System Accounts

Two accounts on the system require attention before any further configuration is done. First, the permissions on the home folder of the initial administrator account

should be changed. Second, any necessary modifications to the root account should be performed.

3.8.1 Restricting Administrator's Home Folder Permissions

The permissions on the home folder of the just-created administrator account allow any user who logs into the system to browse its contents. To change the permissions on the administrator's home folder, issue the following command in a Terminal window, where <adminname> is the name of the account. The 700 permission setting allows only the administrator to read and browse files in his home folder.

```
chmod 700 /Users/<adminname>
```

3.8.2 Securing the Root Account

Mac OS X Server includes a root account like other Unix-based systems. Initially, its password is set to that of the first administrator account. Direct root login should not be allowed because the logs cannot identify which administrator logged in. Instead, accounts with administrator privileges should be used for login, and then the `sudo` command used to perform actions as root. The system uses a file called `/etc/sudoers` to determine which users have the authority to use the `sudo` program, and this file initially specifies that all accounts with administrator privileges may use `sudo`.

To prevent root logins:

1. Log into an administrator account and start the NetInfo Manager application found in `/Applications/Utilities`.
2. Click on the **users** item located in the second column at the top of the NetInfo Manager panel. This will open the list of users in the third column.
3. Click on the **root** item in the **users** column. The root user's properties and any associated values will appear in the bottom panel of the window.
4. Click on the lock in the lower left corner of the NetInfo Manager window. Type an administrator's short name and password into the authentication dialog that appears and click the OK button.
5. If the property **authentication_authority** is listed in the bottom list in the window, click on it to highlight that property.
6. Go to the top of the NetInfo Manager window and click the Delete icon to remove that property and value.
7. Double click on the value associated with the **passwd** property located in that bottom property list, and the value should become highlighted for editing. This value will be a single asterisk if the root password has never been set, and either a string of asterisks or a password hash if a password

has been set for root. (Which of these appear as the value for **passwd** depends upon how the root account was enabled.)

8. Type a single asterisk ("*"), replacing the current value of the **passwd** property.
9. Click the lock icon in the lower left corner of the NetInfo Manager window to re-lock the window.
10. When the Confirm Modification dialog box appears, select Update this copy.
11. Quit the NetInfo Manager application.

There is a timeout value associated with the `sudo` command. This value indicates the number of minutes until the `sudo` command 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 re-entering the password. This value should be changed in the `/etc/sudoers` file. For more information, see the `sudo` and `sudoers` man pages.

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

To change the `/etc/sudoers` file:

1. Edit the `/etc/sudoers` file using the `visudo` command, which allows `/etc/sudoers` to be edited safely. The command must be run as root, so issue the following command:

   ```
   sudo visudo
   ```

   and enter the root password when prompted.
2. In the Defaults specification section of the file, add the following line:

   ```
   Defaults     timestamp_timeout=0
   ```
3. Restrict which administrators are allowed to run the `sudo` command by removing the line that begins with `%admin`, and adding the following entry for each user, substituting the user's id for the word '`user`':

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

   Note that doing this will mean that any time a new administrator is added to a system, that administrator must be added to the `/etc/sudoers` file as described above if that administrator requires the ability to use the `sudo` command.
4. Save and quit `visudo`.

3.8.3 Securing Single-User Boot

On Apple systems running Mac OS X, **Open Firmware** is the software executed immediately after the computer is powered on. This boot firmware is analogous to the BIOS on an x86-based PC. To prevent users from obtaining root access by booting into single user mode or booting from alternate disks, the Open Firmware settings should be altered. For desktop systems, the Open Firmware security mode should be set to **command.** To configure the Open Firmware settings:

1. Boot the machine while holding ⌘-option-O-F (all four keys at the same time) to enter the Open Firmware command prompt.
2. At the prompt, enter the command:

   ```
   password
   ```

3. Enter and verify the password to be used as the Open Firmware password. This password is limited to eight characters. A strong password should be chosen; in this instance, a machine-generated random password would be a good choice. This password should be written down, and secured in the same location as the Master FileVault password. This password will not be needed except for situations where the system must be booted from an alternate disk, such as if the boot disk fails or its filesystem is in need of repair.
4. At the next prompt, enter:

   ```
   setenv security-mode command
   ```

5. To restart the computer and enable the settings, enter the command:

   ```
   reset-all
   ```

6. The system should reboot into the Login Window.

In command mode, the system will boot from the boot device specified in the system's boot device variable and disallow users from providing any boot arguments. To test that the system has been put into command mode as recommended:

1. Close all applications and choose **Restart** from the Apple menu.
2. A confirmation window will pop up. Continue restarting the machine by selecting the **Restart** button.
3. Hold down the key combination ⌘-S while the machine boots.
4. If command mode has been set correctly, the machine will continue booting into the Mac OS X Login Window. Normally, holding down the ⌘-S key combination during a reboot would cause the machine to reboot into single-user mode.
5. If the system did reboot into single-user mode, restart the system by issuing the command `reboot`. Then repeat the previous steps for putting the system into command mode.

Open Firmware protection can be violated if the user has physical access to the machine; If the user changes the physical memory configuration of the machine and then resets the PRAM 3 times (holding down ⌘-option-P-R during boot,) the Open Firmware password will be disabled.

An Open Firmware password will provide some protection although it can be reset if a user has physical access to the machine and can change the physical memory configuration of the machine.

The following Apple Knowledge Base articles discuss the Open Firmware password:

1) **Title:** Setting up Open Firmware Password protection in Mac OS X 10.1 or later; **Article ID:** 106482; **URL:** http://docs.info.apple.com/article.html?artnum=106482

2) **Title:** Open Firmware: Password Not Recognized when it Contains the Letter "U"; **Article ID:** 107666; **URL:** http://docs.info.apple.com/article.html?artnum=107666

Even if a single-user mode boot is successfully initiated by changing the Open Firmware settings, the system can still prevent automatic root login. To require entry of a root password during a single-user mode boot, the console and ttys must be marked as insecure in `/etc/ttys`. In fact, the system will require entry of a special root password, stored in `/etc/master.passwd`. If this remains unset as recommended, then it will be impossible for a user to enter the root password and complete the single-user boot, even if the Open Firmware password protection was bypassed. To perform this configuration:

1. To create a backup copy of /etc/ttys, issue the command:

   ```
   sudo cp /etc/ttys /etc/ttys.old
   ```

2. Edit the `/etc/ttys` file as root, replacing occurrences of the word "secure" with the word "insecure" in the configuration lines of the file. Any line that does not begin with a "`#`" is a configuration line.
3. Exit, saving changes.

Only if the ability to boot into single-user mode is operationally required should a password be provided for the root account in `/etc/master.passwd`. To provide this password:

1. Open the master password file `/etc/master.passwd`.
2. Delete the asterisk following the word "`root`".
3. Open a new terminal window and issue the following command, replacing `<xx>` with two random characters and `<password>` with an appropriate 8-character password:

```
openssl passwd -salt <xx> <password>
```

A hash of the password will be displayed after executing the command.

4. Type or paste the password hash where the asterisk was deleted in step 2.
5. Exit, saving changes.

3.9 Logon Warning Banners

A logon banner can be used to provide notice of the system's ownership, give legal warning to unauthorized users, and remind authorized users of their consent to monitoring. The text displayed in the logon banner should be determined by site policy. Warning banners should be displayed on all systems.

Banners should be provided to anyone logging onto the system. To provide a logon warning banner to any local (GUI) users:

1. Open the file

   ```
   /Library/Preferences/com.apple.loginwindow.plist
   ```

   as an administrator.

2. Immeditately after the <dict> tag, add new lines with a <key> and <string> entry, as show below in bold. The new <key> tag must contain LoginwindowText, but the new <string> can contain whatever warning banner has been indicated by site policy.

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
   <plist version="1.0">
   <dict>
   <key>LoginwindowText</key>
   <string>THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. USE OF THE SYSTEM IMPLIES CONSENT TO MONITORING. ANY UNAUTHORIZED USE OF THE SYSTEM WILL BE PROSECUTED.
   </string>
   ...
   ```

3. Exit, saving changes. The warning banner should appear for the next person logging into the GUI.

To provide a logon warning banner to users logging into remote services on the system:

1. Open the file `/etc/motd` as an administrator.
2. Enter the warning banner that has been approved.
3. Exit, saving changes. The warning banner should appear for the next person logging into a remote service.

3.10 Auditing and Log File Configuration

Apple includes a graphical program, **Console**, to view and maintain log files. Console is found in the `/Applications/Utilities` folder. Upon starting, the console window shows the `console.log` file. Clicking on the **Logs** icon at the top left of the window displays a sidebar that shows other log files on the system in a tree view. The tree includes directories for services such as web and e-mail server software.

In Mac OS X Server, log files are handled by either the BSD subsystem or a specific application. The BSD subsystem handles most of the important system logging, while applications such as the Apache web server handle their own logging. Like other BSD systems, Mac OS X Server uses a background process called `syslogd` to handle logging. A primary decision to make when configuring syslogd is whether to use 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 for any server system.

3.10.1 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 within `/etc/syslog.conf` consists of text containing three types of data: a facility, a priority, and an action. Facilities are categories of log messages. The standard facilities include mail, news, user, and kern (kernel). Priorities deal with the urgency of the message. In order from least to most critical, they are: debug, info, notice, warning, err, crit, alert, and emerg. The priority of the log message is set by the application sending it, not `syslogd`. Finally, the action specifies what to do with a log message of a specific facility and priority. Messages can be sent to files, named pipes, devices, or to a remote host.

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

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

The facility and priority are separated by only a period, and these are separated from the action by one or more tabs. Wildcards ("*") may also be used in the configuration file. The following example line logs all messages of any facility or priority to the file `/var/log/all.log`:

```
*.*                     /var/log/all.log
```

3.10.2 Local Logging

The default configuration in `/etc/syslog.conf` is appropriate for a Mac OS X Server system if a remote log server is not available. The system is set to rotate log files using a **cron** job at the time intervals specified in the file `/etc/crontab`. Rotation entails compressing the current log file, incrementing the integer in the filename of compressed log files, and creating a new log file for new messages (Table 1).

Table 1: Log Files in /var/log

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

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

Details on editing the `/etc/crontab` file can be found by issuing the command `man 5 crontab` in a terminal window. For example, the following line shows the default for running the weekly log rotation script, which is configured for 4:15 AM on the last day of the week, Saturday (Sunday is 0). An asterisk denotes "any," so a line of all asterisks would execute every minute.

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

The following line would change the time to 12:15 PM on Tuesday, when the system is much more likely to be on:

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

3.10.3 Remote Logging

Using remote logging in addition to local logging is strongly recommended for any server system because local logs can easily be altered if the system is compromised. Several security issues must also be considered when making the decision to use remote logging. First, the syslog process sends log messages in the clear, which could expose sensitive information. Second, too many log messages will fill storage space on the logging system, rendering further logging impossible. Third, log files can indicate suspicious activity only if a baseline of normal activity has been established, and if they are regularly monitored for such activity. If these security issues outweigh the security benefit of remote logging for the network being configured, then remote logging should not be used.

The following instructions assume a remote log server has been configured on the network. Configuring Mac OS X Server to act as a remote log server is covered in the System Services chapter. To enable remote logging for a client:

1. Open `/etc/syslog.conf` as root.
2. Add the following line to the top of the file, replacing **your.log.server** with the actual name or IP address of the log server. Make sure to keep all other lines intact:

   ```
   *.*                                    @your.log.server
   ```

3. Exit, saving changes.
4. Send a hangup signal to `syslogd` to make it reload the configuration file:

   ```
   sudo killall – HUP syslogd
   ```

3.11 Disabling Hardware Components

Hardware components such as wireless features and microphones should be physically disabled if possible. Only an Apple Certified Technician should physically disable these components, which may not be practical in all circumstances. The following instructions provide an alternative means of disabling these components by removing the associated kernel extensions. Removing the kernel extensions does not permanently disable the components; however, administrative access is needed to re-load them and restore the capabilities.

Although disabling hardware in this manner is not as secure as disabling hardware physically, it is more secure than only disabling hardware through the System Preferences. This method of disabling hardware components may not be sufficient

to meet site security policy. Consult operational policy to determine if this method is adequate.

1. Open the folder `/System/Library/Extensions`.
2. To remove AirPort support, drag the following files to the Trash:

   ```
   AppleAirPort.kext
   AppleAirPort2.kext
   AppleAirPortFW.kext
   ```

3. To remove support for Bluetooth, drag the following files to the Trash:

   ```
   IOBluetoothFamily.kext
   IOBluetoothHIDDriver.kext
   ```

4. To remove support for audio components such as the microphone, drag the following files to the Trash:

   ```
   AppleOnboardAudio.kext
   AppleUSBAudio.kext
   AudioDeviceTreeUpdater.kext
   IOAudioFamily.kext
   VirtualAudioDriver.kext
   ```

5. To remove support for the iSight camera, drag the following file to the Trash:

   ```
   Apple_iSight.kext
   ```

6. Open the folder `/System/Library`.
7. Drag the following files to the Trash:

   ```
   Extensions.kextcache
   Extensions.mkext
   ```

8. Choose **Secure Empty Trash** from the **Finder** menu to delete the file.
9. Reboot the system.

3.12 Disabling Mac OS 9

The previous major version of the Macintosh operating system, Mac OS 9, does not have many of the security features built into Mac OS X. There are two ways of running Mac OS 9 applications: booting the system into Mac OS 9, and running an application in **Classic Mode**. This mode is an adaptation of Mac OS 9 that runs as an application on a system running Mac OS X. It is not recommended to boot into Mac OS 9 or to use Classic Mode.

By default, Mac OS X Server does not include an installation of Mac OS 9. Some Mac OS 9 files still exist on the system, however, and should be removed. To do this, use the following instructions. Please note that great care must be taken in doing this;

root access is required to do these steps, and incorrectly entering a folder name could result in removal of the Mac OS X operating system or all Mac OS X applications. Note that the files listed below may not appear on all systems.

Following the instructions below will disable Classic Mode and no users will be able to run Mac OS 9 applications.

To remove Mac OS 9 and Mac OS 9 applications and files, do the following as an administrator:

1. Type the following command to remove the Classic icon from the System Preferences panel:

```
sudo rm –rf '/System/Library/PreferencePanes/Classic.prefPane'
```

2. Type the following commands to remove Classic files and directories if they are present on the system. Note that each command should be typed on a single line; they are split across lines here only for readability:

```
sudo rm –rf '/System/Library/Classic/'
sudo rm –rf
     '/System/Library/CoreServices/Classic Startup.app'
sudo rm –rf '/System/Library/
  User Template/English.lproj/Desktop/Desktop (Mac OS 9)'
```

3. Type the following commands to remove additional Mac OS 9 files and directories from the system if they exist:

```
sudo rm –rf '/System Folder'
sudo rm –rf '/Mac OS 9 Files/'
```

Make sure the single quotes (apostrophes) are placed correctly here. If this command is typed incorrectly, it could result in removal of the folder named `System`, which will disable the machine and necessitate a re-installation of the system.

10. Type the following command to remove Mac OS 9 applications if they exist on the system:

```
sudo rm –rf '/Applications (Mac OS 9)'
```

Make sure this command is typed exactly as shown. If the single quotes are not

placed correctly, the `Applications` folder could be deleted.

11. Restart the system.

4. Securing Network Services

Mac OS X Server includes software packages to provide many network services, many of which are based on open-source projects. Although Apple provides configuration tools, completely and securely configuring many of these packages demands familiarization with their project documentation.

4.1 Securing the DNS Service

Mac OS X Server includes an installation of BIND 9.2 (Berkeley Internet Name Daemon) for use as domain name server software. First, the DNS server software should be deactivated if the system is not intended to be a DNS server. Second, some DNS server security configuration is possible through the Server Admin program, and is explained in this chapter. However, detailed setup and secure configuration of the BIND name server is beyond the scope of this document. The following references provide detailed information about tailoring your DNS server to your specific needs:

"Mac OS X Server Network Services Administration for version 10.3 or later." http://www.apple.com/support/server
DNS and BIND, 4th Edition. Paul Albitz, Cricket Liu. O'Reilly and Associates. http://www.oreilly.com/catalog/dns4/index.html
Securing an Internet Name Server. Cricket Liu.

- http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf

FreeBSD Handboook (DNS Section). http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-dns.html

4.1.1 Disable the DNS Service

To disable the DNS service:

1. Open Server Admin.
2. Click DNS in the list for the server you're configuring.
3. Verify that the top of the window says "DNS Service is: Stopped." If not, click the "Stop Service" button.

4.1.2 Basic Security Settings

If the system will be used as a DNS server, some basic security settings can be configured using Server Admin. Unless your site requires them, turn off Zone Transfers and recursive DNS queries as follows:

1. Open Server Admin.
2. Click DNS in the list for the server you're configuring.

3. Click the Settings tab.
4. Uncheck the boxes for “Zone transfers” and “Recursion.”
5. Click Save.

If your site requires recursion, we recommend allowing recursive queries only from trusted clients and not from any external networks. Zone transfers, if needed, should be set up so that they only occur between trusted servers. This requires manually editing the BIND configuration files, which is covered in the references. Also note that using Server Admin after editing the BIND configuration files may overwrite some changes.

Also, make sure that both forward and reverse zones are established and fully populated. If this is not done, any Open Directory server using the DNS service will not work correctly.

4.2 NTP, SNMP, and Macintosh Manager Services

Mac OS X Server includes basic network management services including network time protocol (NTP) server software, simple network management protocol (SNMP) software, and Macintosh Manager server software. Unless they are necessary, they should be disabled. They are all disabled by default, but verification is recommended.

The NTP software is an open-source implementation from http://www.ntp.org and allows Mac OS X Server to provide the current time to clients, so that they may synchronize their clocks. Client systems specify their NTP server in the Date & Time panel in System Preferences. If the NTP service is required, it should be enabled on a single, trusted server within the local network. This service should otherwise be disabled on all servers.

The SNMP software is also an open-source implementation and allows for other systems to monitor and collect data on the state of a Mac OS X server. More extensive documentation is available at the project web page at http://net-snmp.sourceforge.net. Use of this service is not recommended.

The Macintosh Manager server software allows Mac OS X Server to manage Mac OS 9 client systems and is described in Apple’s “Mac OS X Server User Management for version 10.3.3 or later” manual. Use of Mac OS 9 on the network is not recommended, and so this service should be disabled on all servers.

4.2.1 Disable the NTP, SNMP, and Macintosh Manager Services

To disable these services:

1. Open Server Admin.
2. Click the name of the server you're configuring.
3. Click the Advanced Tab under Settings.
4. Uncheck the boxes for "Enable NTP," "Enable SNMP," and "Enable Macintosh Manager" unless they are required.

4.3 DHCP Service

Mac OS X Server includes dynamic host configuration protocol (DHCP) server software, which allows it to distribute IP addresses, LDAP server information, and DNS server information to clients. Using DHCP is not recommended. Assigning static IP addresses eases accountability and mitigates the risks posed by a rogue DHCP server. Even if use of DHCP is necessary, only one system should act as the DHCP server and the service should be disabled on all other systems.

4.3.1 Disable the DHCP Service

To disable the DHCP service:

1. Open Server Admin.
2. Click DHCP in the list for the server you're configuring.
3. Verify that the top of the window says "DHCP Service is: Stopped." If not, click the "Stop Service" button.

4.3.2 Configure the DHCP Service

If using the system as a DHCP server is absolutely necessary, distributing DNS, LDAP, and WINS information is not recommended. To prevent serving this information as part of DHCP:

1. Open Server Admin.
2. Click DHCP in the list for the server you're configuring.
3. Click Settings.
4. In the list that appears, double-click on the subnet you're configuring.
5. Click on the DNS tab.
6. Delete any Name Servers listed.
7. Click on the LDAP tab.
8. Delete any server information that appears.
9. Click on the WINS tab.
10. Delete the WINS information.

11. Click the back arrow on the top right, and repeat from step 4 for any other subnets.
12. Click Save.

4.4 Enabling the Secure Sockets Layer

The Secure Sockets Layer (SSL) is a protocol that allows encrypted network communications, providing protection to data such as e-mail and web transactions. Mac OS X includes SSL support and using SSL is recommended whenever possible. The SSL implementation shipped with Mac OS X is an open-source project called OpenSSL (http://www.openssl.org).

SSL uses public key cryptography to authenticate and encrypt. Public key cryptography involves two keys, one called the public key and the other called the private key. These keys are mathematically linked such that data encrypted with one key can only be decrypted by the other, and vice versa. If a user named Bob publicly distributed his public key, then user Alice could use it to encrypt a message and send it to him. Only Bob will be able to decrypt and read the message, because only he has his private key.

The security of SSL is dependent on SSL certificates, which are files that contain information about a machine and its public key, along with a signature of those items.

In this scenario, Alice still has to verify that the key she has that is supposedly from Bob is really from him. Suppose a malicious user posing as Bob sent Alice his own public key. The malicious user would then be able to decrypt Alice's message, which may have been intended for Bob only.

In order to verify that it's really Bob who is sending Alice his public key, a trusted third party can verify the authenticity of Bob's public key. In SSL parlance, this trusted third party is known as a Certificate Authority (CA). The CA signs Bob's public key with its private key, creating a certificate. Now, anyone can verify the certificate's authenticity using the CA's public key.

This presents something of a chicken-and-egg problem, since a malicious user could also pose as a CA. However, client software includes public keys from well-known CA's, so no network communication with a CA is necessary to verify that the signature inside a server's SSL certificate is authentic.

4.4.1 Obtaining SSL Certificates

If your server must communicate using SSL with external machines out of your control, purchasing SSL certificates from a well-known CA is recommended. The

steps for doing this vary by vendor but are outlined in the "Setting up SSL" section of Apple's "Mac OS X Server Web Technologies Administration" manual. Once the certificates have been obtained, configuration of the services is the same whether they were purchased from a vendor or signed by your own CA.

If you are setting up an internal network and only need to encrypt local traffic, set up a CA to sign SSL certificates for the internal network. The next sections describe this process. While the security is only as good as the security of the CA, in many cases this is sufficient to enable encrypted communication between a web or mail server and their clients. The basic steps to set up an internal SSL-encrypted network are:

- Create a CA.
- Distribute the CA's certificate to client systems.
- Use the CA to sign the certificates the servers will use.

4.4.1.1 Creating a CA to sign certificates

Creating a CA is possible on any system with OpenSSL installed, including Mac OS X. Since the security of your certificates is dependent on the security of the CA, performing these steps on a secure machine is critical. The machine should be physically secure and not connected to any network.

To create a folder to hold the certificate files, open Terminal and execute the following:

```
cd /usr/share
sudo mkdir certs
cd certs
```

To create the CA, generate a key pair as follows:

```
sudo openssl genrsa -des3 -out ca.key 2048
```

This command generates a Triple-DES encrypted RSA public-private key pair called ca.key. The 2048 is the length of the key in bits. OpenSSL will ask for a passphrase for the key upon creating it. Use a strong passphrase and keep it secure; a compromise of this passphrase would undermine the security of your entire certificate system.

Next, the newly created public key is signed to create an SSL certificate that may be distributed to other systems. Later, when we sign other servers' certificates with our CA's private key, any client can then use the CA's SSL certificate (containing its public key) to verify those signatures. When a CA signs a server's certificate with its private key, it means that it is vouching for the authenticity of those certificates. Anyone who can trust the CA can then trust any certificate the CA signs.

To sign the newly created CA's public key to produce a certificate for distribution:

```
sudo openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

When prompted, enter a strong passphrase for the key, as well as these fields:

Country Name:	Organizational Unit:
State or Province Name:	Common Name:
Locality Name (city):	Email Address:
Organization Name:	

These fields should be filled out as accurately as possible, but those that don't apply may be left blank. At least one field must be filled in.

This creates a self-signed certificate called `ca.crt`, using the keys in `ca.key`, which is valid for a year (365 days). This limit may be set to a longer period of time, although this is less secure. The issue is similar to changing passwords regularly; a balance must be found between convenience and security.

We now have a Certificate Authority and are almost ready to start signing other servers' certificates. When signing certificates, OpenSSL looks for keys and related information in directories specified in its configuration file `openssl.cnf`, which is found in `/System/Library/OpenSSL` on Mac OS X systems and frequently in `/usr/share/ssl` on other systems. To create the directories and files where it expects to find them by default, issue the following commands as an administrator:

```
cd /usr/share/certs
mkdir -p demoCA/private
cp ca.key demoCA/private/cakey.pem
cp ca.crt demoCA/cacert.pem
mkdir demoCA/newcerts
touch demoCA/index.txt
echo "01" > demoCA/serial
```

Now the CA is ready to sign certificates for servers, enabling encrypted communications between servers and clients.

4.4.1.2 Creating an SSL Certificate for Web Services

If you've set up your own CA as described in the previous section, you can now sign your own web server SSL certificates. First, a separate certificate must be created for each domain name. For example, if a secure web page exists at www.mypage.net and a secure mail server is at mail.mypage.net, two certificates are needed. This is because the SSL protocol uses the certificate's Common Name field to verify the domain name.

On the machine set up as a CA, generate a key pair for the web server:

```
cd /usr/share/certs
sudo openssl genrsa -des3 -out webserver.key 2048
```

When prompted, enter a strong, unique passphrase to protect the web server key pair.

Next, generate a Certificate Signing Request (CSR) for the CA:

```
sudo openssl req -new -key webserver.key -out webserver.csr
```

Enter the passphrase for the web server key pair and then fill out the following fields as completely as possible:

Country Name:	Organizational Unit:
State or Province Name:	Common Name:
Locality Name (city):	Email Address:
Organization Name:	

The Common Name field is critically important. It must match the domain name of your server exactly (e.g. www.mypage.net) or the certificate will not work. Leave the challenge password and an optional company name blank.

Sign `webserver.csr` as follows:

```
sudo openssl ca -in webserver.csr -out webserver.crt
```

When prompted, enter the CA passphrase to continue and then complete the process.

The certificate files needed to enable SSL on a web server are now in the `/usr/share/certs` directory. As described in the "Securing Web Services" section, some of these files will need to be moved to the web server.

4.4.1.3 Creating an SSL Certificate for E-mail Services

The steps to create SSL certificates for the mail server are similar to those for the web server. If the mail server and web server exist on the same machine and use the same domain name, the same server certificate could be used for both servers. However, this is not recommended.

To create a new mail server certificate, open the Terminal, change to the `/usr/share/certs` directory created in the section "Creating a CA to Sign Certificates," and issue this command to create a key pair for the mail server:

```
sudo openssl genrsa -out mailserver.key 2048
```

This differs from the web server certificate in that it is not encrypted (No -des3 option). The mail server requires an unencrypted key.

Now create the CSR with the mail server key:

```
sudo openssl req -new -key mailserver.key -out mailserver.csr
```

Fill out the following fields as completely as possible:

Country Name:	Organizational Unit:
State or Province Name:	Common Name:
Locality Name (city):	Email Address:
Organization Name:	

The Common Name field is critically important. It must match the domain name of the mail server exactly or the certificate will not work.

Sign `mailserver.csr` as follows:

```
openssl ca -in mailserver.csr -out mailserver.crt
```

The mail server expects the key and certificate inside the same file, so concatenate the key and certificate:

```
cat mailserver.key mailserver.crt > mailserver.pem
```

This creates the `mailserver.pem` file. This file can be moved to the mail server and installed as described in the "Securing E-mail Services" section.

4.4.1.4 Creating an SSL Certificate for LDAP Services

Generating SSL certificates for LDAP services is similar to generating SSL certificates for the web server. Start by generating a private key for the server in the `/usr/share/certs` directory:

```
sudo openssl genrsa -out ldapserver.key 2048
```

Next, a CSR must be generated for the CA to sign:

```
sudo openssl req -new -key ldapserver.key -out ldapserver.csr
```

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 an optional company name blank.

Sign the `ldapserver.csr` request:

```
sudo openssl ca -in ldapserver.csr -out ldapserver.crt
```

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` directory. As described in the "Securing Open Directory Service" section, some of these files will need to be moved to the LDAP server.

4.4.2 Enable Client Support

If you're using self-signed certificates, most user applications will pop up a warning that the Certificate Authority is not recognized. Other software, such as Mac OS X's LDAP client, will simply refuse to use SSL if the server's CA is unknown. The operating system ships only with certificates from well-known commercial CA's. In order to prevent this warning, your CA certificate must be exported to every client machine that will be connecting to the secure server. Each client should do the following:

Copy the self-signed CA certificate (the file called `ca.crt`) onto the client machine. This is preferably distributed via non-rewritable media, such as a CD-R.

1. Double click on the `ca.crt` icon where it was copied onto the client machine. The Keychain Access tool will pop up. Add the certificate to the X509Anchors keychain. Alternatively, issue the command:

```
sudo certtool i ca.crt k=/System/Library/Keychains/X509Anchors
```

Now, any client application that checks against the system's X509Anchors keychain (such as Safari and Mail) will recognize any certificate signed by your CA.

4.5 Securing Open Directory Service

The Open Directory service allows Mac OS X Server to provide directory services such as user authentication. Detailed documentation and configuration advice is available in Apple's "Mac OS X Server Open Directory Administration" guide. The Open Directory service 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 the Open Directory service.

4.5.1 Configure Role

The Open Directory service can act in one of four different roles: Standalone Server, Open Directory Master, Connected to a Directory System, and Open Directory Replica. A Mac OS X Server system that does not participate in a directory domain (and only authenticates users using its own local directory) should have its role set to Standalone Server so that it does not engage in unnecessary network communications. Using the other roles depend on the system's place in the overall network and directory structure. To configure the Open Directory Role:

1. Open Server Admin
2. Click Open Directory in the list for the server you want.
3. Click on the Settings tab.
4. If the role is set to Open Directory Master:
    a. Make sure that only legitimate replicas are listed.
    b. Replicating to clients whenever the directory is modified is recommended.
5. If the role is set to Open Directory Replica, make sure that the intended Master is set.
6. If the role is set to Connected to a Directory System, make sure that the system has joined the appropriate Kerberos realm.

4.5.2 Configure Protocols

The *Open Directory Master* and *Open Directory Replica* roles involve the Open Directory service communicating LDAP information over the network, and these communications should be protected by SSL. After following the instructions of the earlier section "Creating an SSL Certificate for LDAP Services," the required files should be on your own CA. If they were purchased from a commercial CA, the following instructions will apply. From the Open Directory panel in Server Admin, do the following to ready the Open Directory service for SSL:

1. Click on the Settings tab.
2. Click the Protocols button at the top of the pane.
3. At the "Configure:" pop-up menu, choose LDAP settings. Using NetInfo is not recommended.
4. Make sure the "Search base" and "Database" text fields are correct for your site.
5. Place a check in the box for "Use SSL."
6. Certificates and key files need to be specified to support SSL. If you're using a certificate from a commercial Certificate Authority, follow their instructions for handling these files. If you are using self-signed

certificates as discussed in "Creating an SSL Certificate for LDAP Services," this can be accomplished as follows:

a. Copy the files `ldapserver.crt`, `ldapserver.key`, and `ca.crt` from the CA to the /System/Library/OpenSSL/certs directory on the LDAP server. Use a removable medium such as a CD or USB Flash memory; do not copy the files over the network.

b. Enter the location for the `ldapserver.crt` file in the "SSL Certificate" field.

c. Enter the location for the `ldapserver.key` file in the "SSL Key" field.

d. Enter the location for the `ca.crt` file in the "CA Certificate" field.

7. Click Save.

4.5.3 Configure Authentication Policies

If the system is running as an Open Directory Master or Replica, then the directory domain's password policies can be configured through Server Admin. From the Open Directory panel in Server Admin, do the following to configure password policies:

1. Click on the Settings tab.
2. Click on the Authentication button at the top of the pane.
3. In the "Disable accounts section," place a check in the box for "on" and enter a date when the account will no longer be needed.
4. Place a check in the box for "after ____" failed login attempts and enter 3 in the text field or whatever is required by site policy.
5. In the "Passwords must" section, place a check in the box for "be at least ___" characters long and enter 12 in the text field.
6. Place a check in the box for "contain at least one letter."
7. Place a check in the box for "contain at least one numeric character."
8. Place a check in the box for "differ from account name."
9. Place a check in the box for "differ from the last ___ passwords used" and enter 3.
10. Place a check in the box for "be changed every" and set it to 90 days.
11. Click Save.

4.6 Securing Web Services

Mac OS X Server includes an installation of the Apache Web Server version 1.3. It also ships with Apache version 2 for evaluation purposes, but version 1.3 is recommended. First, the web server software should be deactivated if the system is

not intended to be a web server. Second, secure web administration demands scrutiny of some basic configuration settings. Third, SSL encryption should be used to encrypt any sensitive web traffic. Securely configuring all features of the Apache Web Server is beyond the scope of this document. Apple's "Mac OS X Server Web Technologies Administration" manual provides an introduction to basic web services on Mac OS X and security issues involved. The Apache project web page (http://www.apache.org/) provides complete documentation, and the Center for Internet Security (http://www.cisecurity.org) provides an Apache Benchmark and Scoring tool. Basic configuration guidance that can be done using the Server Manager tool is given in this section.

4.6.1 Disable the Web Server

If the system is not intended to be a web server, deactivate web services using the Server Admin tool. On a newly-installed system, the web server should be off by default, but verification is recommended. To deactivate web services:

1. Open Server Admin.
2. Click Web in the list for the server you want.
3. Verify that the top of the Overview window says "Web Service is: Stopped." If not, stop the service by clicking the Stop Service button at the top of the window.

4.6.2 Basic Security Settings

If the system must act as a web server, check some basic security-relevant web server settings:

1. Open Server Admin.
2. Click Web in the list for the server you want.
3. Click Settings.
4. Click Modules.
5. Uncheck all the boxes except for the modules that your site requires.
6. Click Sites.
7. Double-click on your site in the list. A new pane with configuration options for that site should appear.
8. Click the Options tab.
9. Uncheck the boxes for Folder Listing, WebDAV, CGI Execution, and WebMail unless they are required.

See the other resources for more detailed security configuration settings.

4.6.3 Configuring SSL Support

Using SSL to offer a secure communication channel to web visitors requires three separate files:

- A signed server certificate
- The server's private key (used to create the Certificate Signing Request)
- The certificate of the Certificate Authority that signed our Certificate Signing Request

After following the instructions of the previous section “Creating an SSL Certificate for Web Services,” the three necessary files should be located in the CA’s /usr/share/certs directory. If they were purchased from a commercial CA, the following instructions will apply. To ready the web server for SSL, open Server Admin and do the following:

1. Open Server Admin.
2. Click Web in the list for the server you want.
3. Click on the Settings tab.
4. Click on the Sites tab to view a list of sites.
5. Click on the site you want to use SSL, and click on the edit button.
6. In the General Tab, enter the domain name of the site in the Domain Name field (Remember that this should match the Common Name in the site's certificate.)
7. Change the port to 443. This is the default port for SSL communication.
8. Click on the Security tab.
9. Check the "Enable Secure Sockets Layer" checkbox.
10. Enter the passphrase for the server certificate in the Pass Phrase entry box.

We now have to copy the information from the three aforementioned files into the files listed on the Security tab. If you are using self-signed certificates as discussed in “Creating an SSL Certificate for Web Services,” this can be accomplished as follows:

1. Copy the files server.crt, server.key, and ca.key from the CA to the web server. Use a removable medium such as a CD or USB Flash memory; do not copy the files over the network.
2. On the web server, open the server.crt, server.key, and ca.key files with TextEdit. (Hold down mouse button over icon, click Open With, Other... and select TextEdit for each of the files.)
3. Click on the pencil (Edit) icon in the Server Admin window’s Web Security tab next to the Certificate File entry. Copy the entire contents of the server.crt file into the edit window, and click OK.

4. Do the same thing for the server.key file and the ca.crt file, next to the Key File and CA File entries, respectively.
5. In Server Admin, click on the Options tab, and make sure the Performance Cache is disabled for this SSL site. The Performance Cache may cause problems with the SSL authentication.
6. Click Save.

The web server should now accept SSL connections on the port specified.

4.7 Securing E-mail Services

The e-mail services shipped with Mac OS X Server consist of two software packages: Postfix for outgoing e-mail service, and Cyrus for incoming e-mail service. The Postfix software provides an SMTP server that allows users to send e-mail. The Cyrus software provides both IMAP and POP3 servers that allow users to retrieve their e-mail from the server. The following sections cover basic security settings; securely configuring every feature of the Postfix and Cyrus packages is out of scope for this guide. More documentation and configuration advice is available in Apple's "Mac OS X Server Mail Service Administration" guide and the project web pages (http://www.postfix.org and http://asg.web.cmu.edu/cyrus).

4.7.1 Disable Unnecessary E-mail Services

Mac OS X includes support for three e-mail service protocols: IMAP, POP, and SMTP. Turn off support for any of these protocols that is not required. We also recommend using different systems for providing outgoing mail service (SMTP) and incoming mail service (IMAP or POP) where possible. The e-mail services are disabled by default, but verification is recommended. To deactivate unnecessary e-mail services:

1. Open Server Admin.
2. Click Mail in the list for the server you want.
3. Click on the Overview button and verify that the pane says "Mail Service is: Stopped". If not, click Stop Service.
4. Click on the Settings tab.
5. Uncheck "Enable SMTP" if the system will not be used as an outgoing mail server.
6. Uncheck "Enable IMAP" if the system will not be used as an incoming mail server.
7. Uncheck "Enable POP" if the system will not be used as an incoming mail server.
8. Click Save.

4.7.2 Configure SSL Support

If any e-mail services are required, their communications should be protected by SSL. Enabling SSL for incoming (IMAP and POP) and outgoing (SMTP) mail service will encrypt communications between the mail server and its clients, protecting clients from eavesdroppers on the local network.

4.7.2.1 Install Mail Server Certificates

If you're running an outgoing mail service and have decided to act as your own CA as described in "Enabling Secure Sockets Layer," copy the `mailserver.pem` file to the `/etc/postfix/` directory and change its name to `server.pem`. If you've purchased a certificate from a commercial CA, follow their instructions to ensure that the correct information ends up in `/etc/postfix/server.pem`.

If you're running an incoming mail service and have decided to act as your own CA as described in "Enabling Secure Sockets Layer," copy the `mailserver.pem` file to the `/var/imap` directory and change its name to `server.pem`. If you've purchased a certificate from a commercial CA, follow their instructions to ensure that the correct information ends up in `/var/imap/server.pem`. The ownership of the server.pem file must also be changed so that the IMAP and POP server can read it:

```
chown cyrus /var/imap/server.pem
```

4.7.2.2 Enable SSL Support

Now that the certificate and key are in place, enable SSL for mail service as follows:

1. Open Server Admin and click Mail under the server you're configuring.
2. Click Settings.
3. Click on the "Advanced" tab.
4. Select "Require" from the SMTP SSL drop down menu.
5. Select "Require" from the IMAP and POP SSL drop down menu.
6. Click Save.

Three options exist for the server's SSL support: Require, Use, and Don't Use. "Use" will allow both regular and SSL connections. This is better than "Don't use," but "Require" is recommended. Remember that SMTP mail clients must support SSL connections in addition to setting this up on the mail server. On a homogenous Mac OS X network, this isn't an issue since Apple's Mail client supports SSL, but on a heterogeneous network, SSL support on the client side may not exist.

Mail clients must be set up to use SSL connections. Configuring an active mail server in the manner described will cause a loss of service until the clients are reconfigured. Setting the "Use" option for a small period of time to allow clients to switch before "Require" is set may help them avoid a denial of service.

4.7.3 Configure Authentication Support

Authentication support will protect users' passwords as they travel across the network. Although a proper SSL setup will already encrypt the mail client-server communications, using a secure authentication method is also recommended.

1. Open Server Admin.
2. Click on the Mail server button.
3. Click on Settings.
4. Click on the "Advanced" tab.
5. Uncheck all the boxes in the Authentication: section (in the SMTP, IMAP, and POP columns).
6. Select an authentication method. If your system is integrated into a Kerberos realm, place a check in the Kerberos boxes for whichever services (SMTP, IMAP, or POP) your system offers. If your system is not integrated into a Kerberos realm, select CRAM-MD5 in the SMTP and IMAP columns, and APOP in the POP column.
7. Click the "Save" button to apply the changes

4.7.4 Set Account to Receive Problem Reports

An account should be set to receive reports of e-mail problems from Postfix. The Postfix configuration files located in /etc/postfix refer to this address or one of its aliases.

1. Open `/etc/aliases` as root.
2. Change the line reading

   ```
   #root:              you
   ```

   to

   ```
   root:               adminaccount
   ```

   where adminaccount is the name of an administrator account that should receive reports of e-mail problems. It may be desirable to create an account specifically for this purpose. Any of Postfix's configuration files that are set to send mail to root or postmaster should now send mail to the adminaccount specified.

3. To update Postfix to use the new alias, issue the command:

```
newaliases
```

4.7.5 Disable the SMTP Banner

The SMTP banner provides information about the mail server software running on the system that could be useful to an attacker. To remove this information and replace it with a warning banner:

1. Open `/etc/postfix/main.cf` in a text editor.
2. Make sure any lines beginning with `smtpd_banner` are commented out, and add the following line:

```
smtpd_banner = "Unauthorized use is prohibited."
```

4.8 Remote Logging

The remote logging software included with Mac OS X Server is called syslogd (the syslog daemon). It contains features not documented in its man page. A more recent man page that fully describes its features is available at http://www.freebsd.org/cgi/man.cgi?query=syslogd. This service accepts and stores log messages from other systems on the network. In the event that another system is compromised, its local logs can be altered and so the log server may contain the only accurate system records. Remote logging should only be enabled across a trusted internal network or VPN. By default, Mac OS X Server performs only local logging and will not act as a log server. Configuring Mac OS X Server to use another system as a log server is discussed in the Basic Installation and Configuration chapter.

Configuring Mac OS X Server to act as a remote log server involves changing syslogd's command line arguments. Enabling remote logging services requires removal of the -s tag from the syslogd command, which allows any host to send traffic via UDP to the logging machine, which can present security risks. In order to better control what hosts are allowed to send logging message traffic, the -a option should be used to ensure that log messages from only certain IP addresses are accepted. The –a option may be used multiple times to specify additional hosts. The -a option should be followed with an address in the format:

```
ipaddress/masklen[:service]
```

This format is the IPv4 address with a mask bit length. Optionally, the service is a name or number of the UDP port the source packet must belong to. When using this -a option, do not omit the masklen portion, as the default masklen may be very small and the corresponding matching addresses could therefore be almost anything. The default [:service] is 'syslog' and should not need to be changed. For example, match a subnet of 255 hosts as follows:

```
-a 192.168.1.0/24
```

or match a single host like this:

```
-a 192.168.1.23/32
```

It is also possible to specify hostnames or domain names instead of IP addresses, but this is not recommended.

To configure Mac OS X Server as a log server that accepts log messages from other systems on the network:

1. Open `/etc/rc` and locate the line that reads:

```
/usr/sbin/syslogd -s -m 0
```

2. Replacing the address after `-a` with your site's network, change the line to:

```
I/usr/sbin/syslogd –n -a 192.168.1.0/24
```

   The –n option disables DNS lookups.

3. Insert this command as the second to last line of the file, right before the "exit 0" line as illustrated here:

```
killall -HUP syslogd     #re-load configuration
exit 0
```

4.9 Securing Remote Login

The remote login service provided with Mac OS X is Secure Shell (SSH). This service provides access via an encrypted link. Older services such as Telnet or RSH that do not encrypt their communications should never be used as they allow network eavesdroppers to intercept passwords or other data.

4.9.1 Disable Remote Login

If it is not necessary to remotely log into the system or use another program that depends on SSH, then the Remote Login service should be disabled. Programs that depend on SSH for network communications include Server Admin. Disabling Remote Login on a server will prevent remote administration of that server via Server Admin. To disable Remote Login:

1. Open System Preferences.
2. Click on the Sharing icon.
3. Uncheck the "Remote Login" item in the Service list.

4.9.2 Configure OpenSSH

If it is necessary to use SSH, then altering the default settings is recommended. The SSH server configuration file is located at `/private/etc/sshd_config` (and is

also accessible at `/etc/sshd_config` because `/etc` is a symbolic link to `/private/etc`). To implement recommended settings:

1. Open `/private/etc/sshd_config`.
2. Locate the "Authentication" section.
3. To disable root login via SSH (forcing the administrator to use su or sudo to obtain root privileges), change the PermitRootLogin line to:

```
PermitRootLogin no
```

4. To have the SSH server ensure that permissions on users' files and directories are correct before allowing the connection, change the StrictModes line to:

```
StrictModes yes
```

5. By default, SSH allows normal user accounts to login. If it is appropriate to allow only certain users to log in via SSH (e.g. user1, user2, and user3), add the following line to the file:

```
AllowUsers user1 user2 user3
```

6. Alternatively, if it is appropriate to allow all users to login via SSH but deny a few, add the line:

```
DenyUsers user1 user2 user3
```

7. Apple's default configuration file specifies that only version 2 of the SSH protcol is supported. Using only version 2 is strongly recommended, so check that the following line exists in your installation:

```
Protocol 2
```

4.10 Exporting File Systems

Mac OS X Server offers the ability to share files with other computers on the network. Apple's *Mac OS X Server File Services Administration* guide describes this capability and its configuration.

First, file sharing services should be disabled if the system is not to act as a file server. Second, if the system is to act as a file server, file sharing protocols must be chosen and configured for the directories to be shared, which are called "share points." The current protocol choices are Apple File Protocol (AFP), Network File

System (NFS), Microsoft Windows' Server Message Block (SMB), and File Transfer Protocol (FTP). Each of these protocols is appropriate for certain situations.

4.10.1 Disable File Sharing

File sharing services should be disabled unless it is necessary for the system to share files stored on it. To disable file sharing services:

1. Open Workgroup Manager and connect to the server you're configuring.
2. Click the Sharing icon and then click the Share Points tab (which will contain Groups, Public, and Users by default).
3. For each Share Point listed, uncheck "Share this item and its contents" and click Save.
4. Open Server Admin.
5. Click AFP under the Server you're configuring.
6. Click on the Overview button and verify that the pane says "Apple File Service is: Stopped". If not, click Stop.
7. Click FTP under the Server you're configuring.
8. Click on the Overview button and verify that the pane says "FTP Service is: Stopped". If not, click Stop.
9. Click NFS under the Server you're configuring.
10. Click on the Overview button and verify that the pane says "NFS Service is: Stopped."
11. Click Windows under the Server you're configuring.
12. Click on the Overview button and verify that the pane says "Windows Service is: Stopped". If not, click Stop.

4.10.2 Choosing a File Sharing Protocol

If the system is to act as a file server, then share points should be created and configured using Workgroup Manager. Most installations will need only one file sharing protocol, and as few protocols as possible should be used. Limiting the number of protocols used by a system limits its exposure to vulnerabilities discovered in those protocols. Deciding among AFP, SMB, NFS and FTP depends on the client systems and networking needs.

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.

SMB is the native file sharing protocol for Microsoft Windows. It supports authentication but does not support encrypted network transport. SMB may be an appropriate protocol for Windows clients systems when the network between the

server and client is not at risk for eavesdropping. Generally, use of SMB is not recommended.

NFS is a common file sharing protocol for UNIX computers. NFS does not perform authentication of its clients; it grants access based on client IP address and file permissions. Using NFS can be appropriate if the client computer administration and the network are trusted. Generally, use of NFS is not recommended.

FTP should generally not be used for file sharing. The SFTP feature of the SSH protocol should be used instead. SFTP is designed to provide a secure means of authentication and data transfer, while FTP is not. The only situation where FTP is still an acceptable choice is when the system must act as a file server for anonymous users. This may be necessary over wide area networks, where there is no concern for the confidentiality of the data, and responsibility for the integrity of the data rests with its recipient.

4.10.3 Configuring the File Sharing Protocols

Once a protocol is chosen for file sharing, all unnecessary protocols should be disabled. Next, the share point's filesystem permissions should be appropriately restricted and configuration specific to the file sharing protocol should be performed.

4.10.3.1 Deactivate Unnecessary Protocols

After designating a share point, the default settings allow clients to access it using AFP, SMB, and FTP. To deactivate unnecessary file sharing protocols:

1. Open Workgroup Manager and click on the Sharing icon.
2. Click on the Share Points tab.
3. If any share point is not required, uncheck "Share this item and its contents" and click save. The item should disappear from the list of share points.
4. Select each necessary share point and click on the Protocols tab.
5. Using the pop-up menu in the pane, select each of the protocols (Apple File Protocol, Windows File Settings, Network File System, File Transfer Protocol) and uncheck each box for "Share this item using..." unless the protocol is required.

If no share points are shared with a particular protocol, then the service that runs that protocol can be disabled using the Server Admin program. The NFS service automatically stops when no share points specify its use.

4.10.3.2 Restrict File Permissions

Before a directory is shared, its permissions should be restricted to the maximum extent possible.

Permissions on share points set as user home directories are particularly important. By default, users' home directories are set to allow any other user to read its contents. To restrict a user's home directory to allow only that user (i.e. the owner) to read its contents, issue the command:

```
sudo chmod 700 /Users/<username>
```

If necessary, an argument of 750 would allow other members of the group owning the folder to read and search its contents. By default, the staff group is set as the group owner of user directories, and all user accounts are members of this group.

4.10.3.3 Configuring the AFP Server

As it provides both authentication and encryption, the AFP server is the preferred file sharing method for Macintosh or compatible clients. Note that this does not apply to automatically mounted home directories, where only authentication is provided. To configure the AFP Server with recommended settings:

1. Open Server Admin.
2. Select AFP under the Server's name.
3. Click the Settings button at the bottom of the window. The General settings tab should appear.
4. Uncheck the box for "Enable Rendezvous registration,"
5. Uncheck the box for "Enable browsing with AppleTalk."
6. Enter the Logon Greeting according to site policy.
7. Click the Access tab at the top of the pane.
8. For Authentication, choose "Kerberos" if your system is integrated into a Kerberos system. Otherwise, choose Standard.
9. Check the box for "Enable Secure connections."
10. Uncheck the box for "Enable Guest Access."
11. Uncheck the box for "Enable Administration to masquerade as any registered user."
12. Under Maximum Connections, enter the largest expected number for Client Connections.
13. Although Guest access was disabled, enter "1" for Guest Connections to minimize exposure in case it is accidentally re-enabled.
14. Click the Logging tab at the top of the pane.
15. Select "Enable Access Log" to enable logging.
16. Select "Archive every ___ day(s)." Set the frequency according to site policy or operational need.
17. Check the boxes for Login and Logout to include those events in the access log. If operational needs dictate stronger accounting, check the others.

18. Under Error Log, select "Archive every X days." Set the frequency according to site policy or operational need.
19. Click the Idle Users tab at the top of the pane. The following Idle Users settings are suggested, but can be overridden by any operational need:
    - Uncheck the box for "Allow clients to sleep X hours."
    - Check the box "Disconnect idle users after X minutes" and enter a value into the text field to mitigate risk from a system accidentally left unattended.
    - Uncheck the boxes for Guests, Administrators, Registered Users, and Idle users who have open files.
    - Enter a Disconnect Message notice according to site policy.
20. Click on the green "Start Service" button to begin using the file services.

4.10.3.4 Configuring the Windows file services

If any share points are to use the SMB protocol, then the Windows file services server must be activated and configured. Support for the SMB protocol is provided by the open source Samba project, which is included with Mac OS X Server. For more detailed information on configuring the Samba software, see http://www.samba.org. To configure Windows file services with recommended settings:

1. Open Server Admin.
2. In the Computers & Services pane, select Windows found under the Server's name.
3. Click the Settings button at the bottom of the window. The General settings tab should appear.
4. Choose the Role according to operational needs. If the server shares files but does not provide authentication services, then "Standalone Server" is the appropriate choice
5. Fill the text fields appropriately. Leave the Description field blank. It is convention to make the Computer Name match the hostname (minus the domain name). The Workgroup name depends on the configuration of Windows domains on your subnet.
6. Click the Access tab.
7. Uncheck the box for "Allow guest access."
8. For "Client connections:" click the radio button for maximum, and enter the maximum number of client connections expected. After operational use, the Graphs tab can display the actual usage and guide adjustment of the number.
9. Click the Logging tab.

10. Change the Detail: to at least medium in order to capture authentication failures.
11. Click the Advanced tab.
12. Under Services, uncheck Workgroup Master Browser and Domain Master Browser unless these services are operationally required.
13. Select Off for WINS registration.

4.10.3.5 Configuring the FTP Server

If authentication of users is possible, the SFTP portion of the SSH protocol should be used instead of the FTP server to securely transmit files to and from the server. See the Remote Login section for information on configuring SSH.

FTP is only acceptable 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 may be appropriate in some cases. If this capability is not strictly required, it should be disabled.

To configure the FTP Server to provide anonymous FTP downloads **if operationally required**:

1. Open Server Admin.
2. Select FTP under the Server's name.
3. Click the Settings button at the bottom of the window. The General settings tab should appear.
4. In the General section, enter 1 in the text field to Disconnect client after 1 login failures. Even though we will not accept authenticated connections, logins should fail quickly if it is accidentally activated.
5. Enter an e-mail address specially set up to handle FTP administration, e.g. ftpadmin@hostname.
6. Under Access, select Kerberos for Authentication. If a Kerberos server is not set up, that will also effectively block the authentication process.
7. Allow a maximum of 1 authenticated users; the GUI does not allow setting this to 0. (We will later disable any authenticated users.)
8. Check the box to Enable anonymous access.
9. Determine a maximum number of anonymous users and enter the number into the text field.
10. Uncheck the box for Enable MacBinary and disk image auto-conversion.
11. Click on the Messages tab.
12. Check the box for “Show Welcome Message” and enter a welcome message in accordance with site policy.

13. Check the box for "Show Banner Message" and enter a banner message in accordance with site policy. Do not reveal any software information, such as operating system type or version, in the banner.
14. Click on the Logging tab.
15. Check all boxes on this screen. Even though authenticated users will not be allowed to log in, their attempts should be logged in order to take corrective action.
16. Click on the Advanced tab.
17. Set "Authenticated users see:" to FTP Root and Share Points. Although the anonymous user is not really authenticated, his or her FTP root will be the same.
18. Verify that "Authenticated user FTP root:" is set to /Library/FTPServer/FTPRoot.
19. Click Save.
20. Open the folder /Library/FTPServer/FTPRoot and drag the contents (Users, Groups, Public) to the trash.
21. Drag the files into /Library/FTPServer/FTPRoot that you wish to share with anonymous users.
22. Verify that the file permissions on /Library/FTPServer/FTPRoot do not allow public write access.
23. Open the file /Library/FTPServer/Configuration/ftpaccess for editing.
24. Delete any lines (two by default) that begin with `upload`.
25. Insert the following line to prevent advertisement of operating system and version information:

```
greeting terse
```

26. Insert the following lines to prevent any users from authenticating:

```
deny-gid %-99 %65535
deny-uid %-99 %65535
allow-gid ftp
allow-uid ftp
```

4.10.3.6 Configuring the NFS Server

The NFS server included with Mac OS X allows administrators to limit access to a share point based on a client system's IP address. Access to a share point exported via NFS should be restricted to those systems that require it. To restrict access to a share point:

1. Open Workgroup Manager.
2. Click the Sharing icon in the toolbar.
3. Select the Share Point you wish to configure.

4. Select the Protocols tab.
5. In the pop-up menu in the window pane, select NFS Export Settings. Given that the item is to be exported via NFS, "Export this item and its contents" should be checked.
6. Make sure that the Computer list is as restrictive as possible. Exporting only a particular list of clients is recommended. To do this, select "Client" from the pop-up menu and then click "Add" to add each IP addresses. If *every* machine on a particular subnet requires access, then "Subnet" can be selected from the pop-up menu. Selecting "World" is not recommended.
7. Place a check in the "Map Root user to nobody" box. Verify that the selections for "Map All users to nobody" and "Read-only" meet requirements.

4.11 Set up IP Filtering

Mac OS X's built-in IP filtering service (also called the Firewall service) can prevent other hosts from communicating with services running on the system such as the web server, file sharing services, and remote login. Apple's "Mac OS X Server Network Services Administration" (http://www.apple.com/support/server), the ipfw man page, and comments provided in Apple's configuration files in `/etc/ipfilter` provide detailed guidance on the capabilities of the feature. The following recommendations apply to a server offering network services; the recommendations help ensure that the server will offer only the services intended. These instructions do not cover advanced features such as using the IP filtering service to perform network address translation or routing.

The Firewall service can disrupt network communications and its configuration can be tricky to implement. Do not implement recommendations without understanding their intentions or impact.

The default firewall configuration on Mac OS X Server denies access to all but a few TCP services, and allows access to all UDP services. The goal of configuring the firewall is to identify and permit only those hosts and services you would like to allow, and then deny all others. The recommended settings deny all TCP and UDP services except those explicitly allowed.

Performing any server configuration remotely is not recommended, but configuring the firewall service remotely is especially not recommended because of the risk of disabling communications to the remote host.

4.11.1 Configure the IP Firewall Settings

To configure the Firewall Service locally:

1. Open Server Admin.
2. Click Firewall in the list for the server you're logged into.
3. Click Settings.
4. Click on the "any" item in the IP Address Group column to show services available to any other host, which will appear in the right column. These include IGMP, ICMP Echo Reply, Secure Shell (SSH), Server Admin SSL - also Web-ASIP, Remote Directory Access, Server Admin via Server Admin App, and HTTP and HTTPS ports for Tomcat.
5. Uncheck all of these services, unless you specifically need to offer them to any other host. If you want to offer them only to hosts on your network, still uncheck them here – the next step involves creating rules for other machines on the LAN. This includes the items for Server Admin if you're running it locally as recommended.
6. If you want to allow services to only machines on a particular subnet (such as your local network), create a new IP Address Group in the left column. By default, Apple provides two address groups (named 192.168-net and 10.0.0-net). If these do not fit your network needs, edit or delete them.
7. Check the boxes to allow services for your new IP Address group in the right column.
8. Select the Advanced tab.
9. Uncheck all the boxes marked "deny." These explicit denials will be handled by a rule we'll add later.

10. Keeping the Server Admin program open, add the following lines to `/etc/ipfilter/ipfw.conf` (substituting `$MY_IP`, `$TIME_SERVER`, and `$DNS_SERVER` appropriately):

```
add 02000 allow ip from $MY_IP to any out
#this allows our system to send packets out

add 03000 allow icmp from any to any
#allow icmp messages (e.g. pings) in and out

add 03500 allow udp from $DNS_SERVER 53 to $MY_IP in
#accept packets from our DNS server

add 03600 allow udp from $TIME_SERVER 123 to $MY_IP in
#accept packets from our NTP server

add 65500 allow tcp from any to any established
#accept TCP packets from other hosts once connection est'd

add 65534 deny log ip from any to any in
#deny and log all other packets
```

11. If your system is hosting a UDP-based service, add rules as needed. In the examples below, substitute $MY_CLIENTS with an address or subnet that represents the clients you wish to serve.

```
add 03700 allow udp from $MY_CLIENTS to $MY_IP 123 in
#this permits our system to answer NTP requests

add 03800 allow udp from $MY_CLIENTS to $MY_IP 631 in
#this permits our system to answer IPP printing requests

add 03900 allow udp from $MY_CLIENTS to $MY_IP 2049 in
#this permits our system to act as an NFS server

add 04000 allow udp from $MY_CLIENTS to $MY_IP 514 in
#this permits our system to receive syslog messages
```

12. Save and close `/etc/ipfilter/ipfw.conf`.
13. Switch back to Server Admin.
14. Click the Save button.
15. Click the "Start Service" button to active the firewall.

The firewall rules will need to be updated for any network service you enable and wish to offer to other systems. If the rules are not properly updated, network services will not be available to other systems. Most of these services can be enabled using the Server Admin tool. For those which cannot be enabled that way, an entry should be added to `/etc/ipfilter/ipfw.conf` allowing the type of traffic needed for that service.

5. User and Client Management

Mac OS X Server's Workgroup Manager program allows administrators to enforce system settings on a user, group or computer level. Apple's "Mac OS X Server User Management for version 10.3.3 or later" manual provides detailed instructions on this process, including the important planning stages. The configuration advice below assumes familiarity with Apple's documentation, which describes the process of creating appropriate users, groups, and computer lists using the Workgroup Manager. Apple's documentation also describes how the settings created for the user, group, and computer levels can interact.

5.1 Recommended Account Settings

Many settings relating to new user, group, and computer accounts are particular to the needs of the site. However, the following settings are recommended when using Workgroup Manager to create new accounts. The Presets feature as described in the Apple documentation can also be used to ensure uniform settings and avoid configuration errors.

5.1.1 User Account Settings

In the Basic tab:

- When creating short names, make certain to avoid duplicates anywhere in your directory system as recommended in the Apple documentation.

The password should be at least 12 characters, not be found in a dictionary, and contain mixed case, numbers, and special characters.
Uncheck "User can administer the server" unless required.
Uncheck "User can administer this directory domain" unless required. If this privilege is required, click the Privileges button and restrict the user's ability to manage computers, groups, and users to the minimum required.
If the user should not be able access the server remotely from a command line, uncheck the box for "log in."

In the Advanced tab:
Uncheck the box for Allow simultaneous login. (This cannot be disabled for users with NFS home directories.)
The User Password Type should be set to Open Directory. Using Crypt Password type is not recommended.
Click the Options… button.
Under Disable login, check the box for "on date" and enter a date when the user will no longer need the account. For military personnel, a logical choice might be a transfer date. In a school environment, a logical choice may be a graduation date for a student. Check the box for "if account is inactive for _ days" and enter a number of

days that would indicate the user no longer needs the account. Check the box for "after _ failed attempts" and enter 3 or whatever is required by site policy.
Check the box for Minimum password length and enter 12 in the text field.
Check the box for "Allow the user to change the password."
Check the box for "Require a change at next login" to force the user to select a password at his first login to replace whatever password the administrator initially assigned.
Check the box for "Require a change every _ days" and enter 90 in the text field or whatever is required by site policy.

In the Home tab:
Enforcing a disk quota is recommended to prevent users from attempting a denial of service by filling the home volume. Select the home directory in the list and enter an appropriate value for Disk Quota.

In the Mail tab:
Click None unless the user will use this account to receive mail.
Using the Forward option is not recommended.
If Mail is to be enabled for the account, select only the Mail Access protocol (IMAP only or POP only) to be used.

5.1.2 Group Account Settings

Groups should be created to handle users with similar access needs. For example, creating a separate group for each office would allow an administrator to specify that only members of a certain office can log into certain computers.

5.1.3 Computer Account Settings

Every computer on the network should be a member of a Computer List. Computers on the network that are not assigned to a Computer List are treated as a member of the "Guest computers" list.
After creating and populating computer lists in the List pane, restrict the groups able to log into each computer:
Click on the Access tab.
Click "Restrict to groups below" and add only the groups that should have access to the computer.
Deselect "Allow users with local-only accounts" depending on site policy.

5.2 Recommended Preferences Settings

Workgroup Manager allows for the configuration and enforcement of preferences at the user, group, and computer levels. The final set of preferences a user experiences is a combination of these. Chapters 8 and 9 of Apple's "Mac OS X Server User Management" guide provide a complete explanation, but generally user preferences override computer settings and computer settings override group settings. Setting

these preferences at all levels is recommended in case one level is accidentally left unset. Preferences must be applied to each computer list, group account, and user account, although applying preference settings to multiple computers, groups, or accounts is possible. Preferences can be set for Applications, Classic, Dock, Energy Saver, Finder, Internet, Login, Media Access, Mobile Accounts, Printing, System Preferences, and Universal Access. Security recommendations for Applications, Finder, Login, and Media Access are described below.

5.2.1 Applications

Applications preference management is designed to restrict users from executing some programs. In the Applications pane for each computer list, group, and user account:
If this feature is required, click the "Always" radio button in the "Manage these settings" list. If it's not needed, click "Not managed" and skip to the next section.
Build the list of allowed or restricted applications as needed.
Uncheck the box for "User can also open applications on local volumes."
Uncheck the box for "Allow approved applications to launch nonapproved applications."
Uncheck the box for "Allow Unix tools to run."

5.2.2 Finder

Finder preference management controls behavior of Mac OS X's graphical file manager. In the Finder pane for each computer list, group, and user account:
Click the Preferences tab.
Click the "Always" radio button in the "Manage these settings" list.
The Preferences tab in the window pane should be selected.
"Use normal Finder" should be selected. Only click "Use Simplified Finder to limit access to this computer" if the system is to be used as a kiosk or some other public terminal.
Check the box for "Always show file extensions."
Click the Commands tab.
Survey the commands listed and determine if they should be restricted. If so, click the "Always" radio button in the "Manage these settings" list. Unchecking the boxes for Restart and Shut Down is recommended to protect availability in any environment where multiple users may be logged into a Server.

5.2.3 Login

Login preference management controls behavior of the login screen that appears on client systems. Some of its setting can be applied only to Computer Lists. In the Login pane for each computer list, group, and user account:
Click the Login Items tab.
Click the "Always" radio button in the "Manage these settings" list.
Add any anti-virus or integrity checking software to be run upon user login.

Uncheck the box for “User may press Shift to keep items from opening” to prevent users from disabling any automatic launches.
Click the Login Options tab.
Click the “Always” radio button in the “Manage these settings” list.
For “Display Login Window as:” select “Name and password text fields.”
Uncheck the box for “Show Restart Button in the Login Window.”
Uncheck the box for “Show Shut Down Button in the Login Window.”
Uncheck the box for “Show password hint after 3 attempts to enter a password.”
Uncheck the box for “Enable Auto Login Client Setting.”
Uncheck the box for “Allow users to log-in using “>console.”
Uncheck the box for “Enable Fast User Switching.”
Click the Auto Log-Out tab.
Click the “Always” radio button in the “Manage these settings” list.
Uncheck the box for “Log out users after: ___ minutes of activity.” This feature is not recommended.

5.2.4 Media Access

Media Access preference management allows control over CD/DVD and other drives. If use of the CD/DVD drive or external disks such as USB flash drives or FireWire drives should be restricted, then apply the following settings in the Media Access pane or each computer list, group, and user account:
Click the “Always” radio button in the “Manage these settings” list.
Click the Disc Media tab.
Uncheck the boxes that allow CDs & CD-ROMs, DVDs, and Recordable Discs if these items should not mounted by users.

- Click the Other Media tab.

Uncheck the box for External Devices if these items should not be mounted by users.

5.2.5 Mobile Accounts

The Mobile Accounts feature allows users to log into systems that may not always be connected to the network. Unless operational need exists, this feature should be disabled on clients. To do so, in the Mobile Accounts pane for each computer list, group, and user account:
Click the “Always” radio button in the “Manage these settings” list.
Uncheck the box for “Create Mobile Account at login.”

5.2.6 System Preferences

Users can be limited to seeing only certain items in the System Preferences program on client systems. Access to any security-relevant client settings should be restricted. To allow users access to personalization items but hide all others, in the System Preferences pane for each computer list, group, and user account:
Click the “Always” radio button in the “Manage these settings” list.
Click the “Show None” button.

Check the boxes for Appearance, Dock, Exposé, Security, Keyboard & Mouse, and Universal Access. Desktop & Screen Saver should remain unchecked in order to enforce automatic activation of the screen saver, although this also prevents changing the Desktop picture.

6. References

1. Mac OS X Maximum Security; Ray, John, and Ray, Dr. William C.; Sams Publishing; 2003
2. Mac OS X Panther Unleashed; Ray, John, and Ray, Dr. William C.; Sams Publishing; 2004
3. Inside Mac OS X, "System Overview," Apple Computer, Inc., 2001-2002
4. Firewalls and Internet Security. William R. Cheswick and Steven M. Bellovin. Addison-Wesley, 1994.
5. "Apple Federal Smart Card Package Installation and Setup Guide;" Apple Computer, Inc.; 2003
6. "The Mac OS X File System;" Mac OS X Reference Library. Apple Computer, Inc; March 26, 2004.
7. Joel Rennich. "The Great Big Mac OS X Panther Server and SSL article." http://www.afp548.com/Articles/Panther/sslinfo.html
8. Apple Computer. "Mac OS X Server Mail Service Administration for version 10.3 or Later." http://www.apple.com/support/server
9. Apple Computer. "Mac OS X Server Web Technologies Administration for version 10.3 or later." http://www.apple.com/support/server
10. Apple Computer. "Mac OS X Server Network Services Administration for version 10.3 or later." http://www.apple.com/support/server
11. Apple Computer. "Mac OS X Server File Services Administration for version 10.3 or later." http://www.apple.com/support/server
12. Apple Computer. "Mac OS X Server User Management for version 10.3 or later." http://www.apple.com/support/server