Apple OS X 10.8 (Mountain Lion) Security Baseline

Settings

Install Mac OS X using Mac OS Extended Journaled disk format

This type of file system is the most compatible and supports all of the built-in security features of Mac OS X.

Review and remove any unnecessary applications or packages

Unneeded software unnecessarily increases the attack surface of the system. IF there is no need to have a particular piece of software installed, removal will reduce its potential for system compromise.
Remediation: Use the appropriate method recommended by the vendor to remove unneeded software. If there is no simple way to remove all component parts from the Operating System a clean install or re-image may be necessary.

Do not transfer confidential information in Setup Assistant

The Setup Assistant will prompt the user for name, address, phone number, e- mail address, and other information. If you don't want personal information transferred to Apple, skip this step.
Remediation: In the Registration Information screen, press Command-Q to quit. Click the "Skip" button to bypass the registration process.

Create administrator accounts with difficult-to-guess names

Simple names like "Administrator" or "Admin" are easy to guess, and provide an attacker some information needed to break into a system. Use a difficult-to-guess name for accounts with administration privileges to the Mac

Remediation: When creating the first account in the Setup Assistant, use a difficult-to-guess name.
Additional Info: This applies to both the long name and short name, either of which may be used to log in to the computer through various login mechanisms. The short name is likely to have the widest exposure. The short name for an account cannot be changed after creation.

Create complex passwords for administrator accounts

Passwords are the primary protection against unauthorized access. Accounts with administrative privileges are the most important to protect. Therefore, using a complex password for these accounts is very important.

Caveats: A complex password may be difficult to remember, so some users will write them down. If the password is written down, it should be kept is a safe place, preferably sealed in an envelope and locked up.

Remediation: Apple provides a Password Assistant in the dialogs used to set password. When setting a password, click on the key icon to the right of the New Password field to display the assistant. Make sure the password for the administrator account shows a quality of green. Make sure the quality meter is about halfway across or more. Alternatively, use a password that is at least 15 characters, and three of the following four items. Make sure the password does not contain a name or word found in the dictionary. Local passwords should not be reused on other devices for other purposes. Passwords and devices will be compromised, unique passwords reduce the risk.
Uppercase letter
Lowercase letter
Punctuation characters
Numbers
Additional Info: If you are color blind you may not be able to determine the quality of the password from the password assistant. However, numeric password quality information may be retrieved by hovering the cursor over the quality meter.
The pwpolicy tool can be used to enforce password policies in Mac OS X directory services, but the policies do not apply to administrator-level users.

Do not enter a password-related hint

A password hint will help you remember your password, but may also help an attacker to guess your password.

Caveats: The absence of a password hint may make remembering a password more difficult. Additionally, if using FileVault, not setting a hint may not allow a user to use a Master Password to reset a user account password.
Remediation: In the System Preferences: Accounts: Change Password dialog, enter the appropriate hint.
Additional Info: Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

Create an access warning for the login window

Displaying an access warning that informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored, may reduce a casual attacker’s tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker’s knowledge of the system’s private status, acceptable use policy, and authorization requirements.

A banner text that can be used for systems, when an approved banner text does not already exist, is set with the following command (with appropriate privileges):

```
defaults write /Library/Preferences/com.apple.loginwindow \
LoginwindowText "Warning! This is a Name of the Organization
Computer. This system is for the use of authorized users only. By
accessing and using this computer system you are consenting to
system monitoring, including the monitoring of keystrokes.
Unauthorized use of, or access to, this computer system may
subject you to disciplinary action and criminal prosecution."
```

Note that the above 342 byte standard warning banner text exceeds the 256 character display on the locked screensaver, though it displays correctly on the initial user login screen.

Audit: Audit this setting with the command:

```
defaults read /Library/Preferences/com.apple.loginwindow \
LoginwindowText
```

… and verify the appropriate banner text is printed.

Use the following steps to create a Login window banner that requires a user to acknowledge:
Create a document named PolicyBanner that contains your banner (.txt, .rft,rtfd format).
Copy the PolicyBanner file to the /Library/Security/ folder.

Scoring Status: Scorable

Create an access warning for the command line

There are two common ways to login to a Mac using the command line, bypassing the GUI login window: FTP and SSH. Displaying an access warning that informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored, may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements. Use an appropriate warning message for your environment that has been set by policy or common practice.

A banner text that can be used for systems is set with the following command (with appropriate privileges):

```
defaults write /Library/Preferences/com.apple.loginwindow \
LoginwindowText "Warning! This is a Name of the Organization
Computer. This system is for the use of authorized users only. By
```

```
    accessing and using this computer system you are consenting to
    system monitoring, including the monitoring of keystrokes.
    Unauthorized use of, or access to, this computer system may
    subject you to disciplinary action and criminal prosecution."
```

Caveats: The banner will be displayed before the user logs in. This may interfere with scripted logins.
Remediation: Create a text file with the login text. This is commonly done in /etc/motd for SSH and /etc/ftpwelcome for FTP.

For SSH, edit /etc/sshd_config (using sudo) and add the line:

```
    Banner /etc/banner
```

Where /etc/banner is the path to your login banner text file.
Audit

Run the following commands to determine if the banner text is set:

```
cat /etc/sshd_config | grep Banner
```

If there is a valid entry for Banner, cat the path show and view the results.
Additional Info
see `man sshd_config`

Scoring Status: Scorable

Secure Home Folders

By default the Mac is set up to allow every user to see into the top level of the home folder of other users. This allows user to drop files into the "Drop Box" folders of other users. This also allows users to see newly-created files and folders in the top level of other users' home folders but not within the standard subfolders such as "Documents" and "Library." This access to the top of other users' home folders may not be desirable. To resolve this potential revelation of sensitive information, permissions should be set on home folder to restrict

Scoring Status: Scorable
Caveats: If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.
Remediation: Open Terminal and enter:

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

where <username> is the name of each user. This command has to be run for each user account with a local home folder.
Audit: Run the following command:

```
ls -l /Users/
```

verify that each user home folder looks like drwx------

Turn on file extensions

By making the file extension visible, you can determine the type of file it is and the application it is associated with. It is fairly simple for malicious code or unapproved software to appear as if it is something other than what it is. File Types should be visible

Caveats: Users may prefer not seeing extensions in their environment
Remediation:
1. Open Finder.
2. From the Finder menu, select Preferences.
3. Click Advanced and select the “Show all filename extensions” checkbox.

Create an administrator account and a standard account for each administrator

An administrator account should rarely be used. In most cases when administrative privileges are needed, the Mac will prompt the user for a user name and password. There are some operations where logging in as an administrator is necessary, but these are rare.
The reason to not regularly use an administrator account for daily operations is security. Many operations that affect security can be accomplished without a password when an administrator is logged in. When logged in as a standard user, very few, if any, of the operations that affect the entire computer are possible without authentication to obtain elevated privileges.

Caveats: Administrators have unrestricted write/delete access to various directories, including /Applications and /Library. Administrators, by default, can escalate themselves to have access to any directory on the computer. Care should be given when granting a user administrative access.
Remediation: Do not log in with an administrator account unless necessary.
Audit: Open System Preferences: Accounts and verify there is a regular user account for each administrator.
Additional Info: If administrator rights need to be controlled, consider granting specific sudo rights to individual users as needed.
In larger environments, you may wish to grant administrator rights only to directory service-based groups.

Use a standard or managed account for each non-administrator

A non-administrator should not need administrator privileges on the Mac, so use a standard (or managed, if using Mac OS X Server or Parental Controls) account for these users.

Caveats: Standard users have reduced rights which may affect their ability to alter things on the computer. Standard users cannot install software in the /Applications folder and cannot change various System Preferences, including creation and modification of network settings or the computer's time zone. Standard users can still make some changes, such as switching between administrator-defined network locations.

OS X does not have extensive controls on password management for a system that is not tied to an external Directory System such as Active Directory. Complexity requirements and password expiration for Administrators controls have often been incomplete.

Remediation: Do not give the "Allow user to administer this computer" right to standard users in System Preferences: Accounts.

Additional Info: If you need to grant specific rights to non-administrator users, such as the ability to change time zones, consult the Apple support knowledge base. Some of these rights can be changed in the authorization rights database, /etc/authorization, and Apple does provide articles for common ones.

Use Password Assistant to help generate complex passwords

Passwords are the primary protection against unwanted access.

Caveats: A complex password may be difficult to remember, so some users will write them down. If the password is written down, it should be kept is a safe place, preferably sealed in an envelope and locked up.

Remediation: Apple provides a Password Assistant in the dialogs used to set password. When setting a password, click on the key icon to the right of the New Password field to display the assistant. Make sure the password for the administrator account shows a quality of green. If you are color blind you may not be able to determine the quality of the password from the Password Assistant. Make sure the quality meter is about halfway across or more, or hover over the meter to see its calculated entropy value in a tooltip. For the entropy value, higher is better.

Do not enable the "root" account

The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. In the UNIX/Linux world, the system administrator commonly uses the root account to perform administrative functions. On a Mac, root should not be enabled. In any circumstance an administrator can escalate privileges using the sudo command (use -s or -i to get a root shell).

By default the root account is not enabled on a Mac OS X client computer. It is enabled on Mac OS X Server.

Caveats: UNIX/Linux system administrators need to learn to use sudo -s instead of su -. Also, sudo on the Mac is not Kerberized, but can be with a free third party PAM module.

Remediation: Nothing specific; just don't enable root using the Directory Access program (in /Applications/Utilities/), with the CLI passwd command via sudo, or with the Reset Password utility on the installer DVD.

Audit: Open /Applications/Utilities/Directory Utility program and verify root is disabled.

Alternatively, run the following command:

```
dscl . -read /Users/root AuthenticationAuthority
```

The result should be:

No such key: AuthenticationAuthority

Additional Info: The root password, like those of other local user accounts, can still be reset when using the Password Reset Utility on the Mac OS X Install DVD.

The AuthenticationAuthority attribute could also contain ;DisabledUser; which would prevent logins by the account.

Scoring Status: Scorable

Repair disk permissions after installing software or software updates

Sometimes file permissions get set differently from the desired permissions. A number of reasons might cause this, and most are beyond the control of the user.

Every time a package is installed, the package leaves a receipt that tells the computer what files were installed and what their permissions on disk should be.

Using the repair permissions feature of Disk Utility, the permissions of most program files can be reset to the desired values.

Caveats: If custom permissions were set on items in /Applications or /Library, these permissions may need to be reset.

Remediation:

1. Open Applications: Disk Utility.
2. Select the startup disk in the left panel. 3. Select the First Aid tab.
4. Click on the Repair Permission button

Alternatively the command can be run from Terminal:

```
diskutil repairPermissions /
```

Permissions can be repaired when started up from a Mac OS X Install DVD, but Apple recommends running it from a fully-updated Mac OS X system instead.

Additional Info: Apple recommends running repair permissions from an up-to-date system disk, rather than the system installer DVD.

http://docs.info.apple.com/article.html?artnum=25751

If the system is not maintained by a configuration management tool that manages permissions, a good best practice is to schedule a permission repair to occur at least monthly. Tools like launchd can be used (use Lingon as a GUI front end for launchd). Also, the command line above can be placed in the file /etc/monthly.local and the command will be executed monthly (/etc/weekly.local will execute the command weekly).

User Settings

Users & Groups Preferences

Change initial password for the system administrator account

If you did not set the initial password to the Mac, the password should be changed for all accounts, including the administrator account, as soon as possible. If the initial admin account is not needed, the account should be deleted.

Remediation: In System Preferences: Accounts, select the user, then change the password or delete the account if not needed.
Additional Info: At least one admin account is required, although it does not necessarily need to be enabled or have a known password at any given time. The admin account could be disabled to prevent logins. Or, its password could be set to a strong, highly complicated password that is forgotten and not used. In such cases, you would need to re-enable the account or change its password before use.
It should also be noted that an attacker who has the ability to remove the /var/db/.AppleSetupDone file can restart the computer and create a new administrator account from the Mac OS X Setup Assistant. The. AppleSetupDone file determines whether the system runs the Setup Assistant or not.

Disable automatic login

Having a computer automatically log in bypasses a major security feature (the login) and can allow a casual user access to sensitive data in that user's home directory and keychain.

Remediation: In System Preferences: Accounts, Login Options, disable Automatic Login.
Note: Automatic login can also be disabled in System Preferences: Security.
Alternatively, run the following command

```
sudo defaults write \
/Library/Preferences/.GlobalPreferences \
com.apple.userspref.DisableAutoLogin -bool yes
```

Audit: Open System Preferences: Accounts, Login Options, and verify Automatic Login is disabled.
Alternatively, run the following command:

```
defaults read /Library/Preferences/.GlobalPreferences \
com.apple.userspref.DisableAutoLogin
```

Make sure the value returned is 1.

Scoring Status: Scorable

Display login window as name and password

Displaying the names of the accounts on the computer may make breaking in easier. Force the user to enter a login name and password to log in.

Caveats: Users will need to remember their login name.
Remediation: In System Preferences: Accounts, Login Options, select Name and Password Alternatively, run the following command

```
sudo defaults write \
/Library/Preferences/com.apple.loginwindow \
SHOWFULLNAME -bool yes
```

Audit

Open System Preferences: Accounts, Login Options, and verify Name and Password is selected.

Alternatively, run the following command:

```
defaults read \
/Library/Preferences/com.apple.loginwindow SHOWFULLNAME
```

Make sure the value returned is 1.

Scoring Status: Scorable

Disable “Show password hints”

Password hints can give an attacker a hint as well, so the option to display hints should be turned off. If your organization has a policy to enter a help desk number in the password hints areas, do not turn off the option.

Caveats: Might make remembering a password more difficult. If using FileVault, not setting a hint may not allow a user to use a Master Password to reset a user account password.

Remediation: In System Preferences: Accounts, Login Options, make sure the “Show password hints” checkbox is off.

Alternatively, run the following command

```
sudo defaults write \
/Library/Preferences/com.apple.loginwindow \
RetriesUntilHint -int 0
```

Audit

Open System Preferences: Accounts, Login Options, and verify “Show password hints” checkbox is off.

Alternatively, run the following command:

```
defaults read \
/Library/Preferences/com.apple.loginwindow \
RetriesUntilHint
```

Make sure the value returned is 0.

Scoring Status: Scorable

Disable “Allow guest to log into this computer”

The Guest account allows a guest to log in to a Mac and use all of its services. When the guest logs out, the Mac clears most of whatever the guest did on the Mac. This allows one person to let another borrow the computer for a short period, and still protect information in other accounts on the Mac.

The usage of a Guest account may give the Mac owner a false sense of security. If the guest has physical access to the Mac and the owner is not present, the guest could gain full access to the Mac. That said, use of the Guest account allows for quick and moderately safe computer sharing.

Remediation: In System Preferences: Account, click on the Guest user.
Make sure the “Allow guests to log into this computer” is not checked.
Alternatively, run the following commands:

```
sudo dscl . -create /Users/Guest \
AuthenticationAuthority ";basic;"
sudo dscl . -create /Users/Guest passwd "*"
sudo dscl . -create /Users/Guest UserShell \
"/sbin/nologin"
```

Audit: Run the following command

```
dscl . -read /Users/Guest AuthenticationAuthority
```

The result should be:
AuthenticationAuthority: ;basic;
Additional Info: By default, the guest account is enabled for access to sharing services, but is not allowed to log in to the computer.
The guest account does not need a password when it is enabled to log in to the computer.

Scoring Status: Scorable

Disable “Allow guests to connect to shared folders”

If files need to be shared, a dedicated file server should be used. If file sharing on the client Mac must be used, then only authenticated access should be used. Guest access allows guest to access files they might not need access to.
Remediation: In System Preferences: Account, click on the Guest user.
Make sure the “Allow guests to connect to shared folders” is not checked.
Alternatively, run the following commands:
For AFP sharing:

```
sudo defaults write \
/Library/Preferences/com.apple.AppleFileServer \
guestAccess -bool no
```

for SMB sharing:

```
sudo defaults write \
/Library/Preferences/SystemConfiguration/com.apple.smb.serv
er \
AllowGuestAccess -bool no
```

Audit
In System Preferences: Account, click on the Guest user.
Make sure the “Allow guests to connect to shared folders” is not checked.
Alternatively, run the following command:
For AFP sharing:

```
defaults read
/Library/Preferences/com.apple.AppleFileServer guestAccess
```

for SMB sharing:

```
defaults write \
/Library/Preferences/SystemConfiguration/com.apple.smb.serv
er \
AllowGuestAccess
```

Make sure the results are 0.

Additional Info

This setting is not enabled by default in Snow Leopard, but the sharing services themselves are all turned off.

The guest account does not need a password for access to shared services when it is enabled.

Scoring Status: Scorable

AirPort Preferences

Enable Show AirPort Status in Menu Bar

If an Airport or other wireless card is installed, show the AirPort status in the menu bar so that user can quickly determine if AirPort is on or off. If on, the user can quickly turn it off if AirPort interface should be off.

Remediation: In System Preferences: Network, select the Airport interface, then click the Advanced button. Turn on Show AirPort status in menu bar.

Audit: In System Preferences: Network, select the Airport interface, then click the Advanced button. Verify Show AirPort status in menu bar is on.

Additional Info

AirPort is Apple’s marketing name for its 802.11b/g/n/ac wireless interfaces.

Bluetooth Preferences

Show Bluetooth status in menu bar

By showing the Bluetooth status in the menu bar, a small Bluetooth icon is placed in the menu bar. This icon quickly shows the status of Bluetooth, and can allow the user to quickly turn Bluetooth on or off.

Remediation

In System Preferences: Bluetooth, turn Show Bluetooth Status In Menu Bar on.

Disable Bluetooth internet connection sharing

Bluetooth internet sharing can expose a Mac and the network to certain risks and should be turned off.

Remediation: In System Preferences: Bluetooth, Advanced options, turn off “Share my internet connection with other Bluetooth devices”

Alternatively, run the following commands:

```
sudo defaults write \
/Library/Preferences/com.apple.Bluetooth \
PANServices -int 0
sudo killall -HUP blued
```

Audit: In System Preferences: Bluetooth, Advanced options, verify “Share my internet connection with other Bluetooth devices” if off
Alternatively, run the following commands

```
defaults read /Library/Preferences/com.apple.Bluetooth
PANServices
```

and make sure the value returned is 0.
Additional Info: This setting is turned off by default in Snow Leopard.

Scoring Status: Scorable

If Bluetooth is used, turn off “Discoverable” when not needed

When Bluetooth is set to "discoverable" mode, the Mac sends a signal indicating that it's available to "pair" with another Bluetooth device. When in discoverable state an attacker could gain access to data on the Mac. Use discoverable mode when “pairing” a Bluetooth device to the Mac, but once the “pairing” is complete, turn discoverable mode off.

Remediation: In System Preferences: Bluetooth, turn Discoverable off when not actively “pairing” a Bluetooth device.

Date & Time Preferences

Enter correct time settings

Having the correct date, time, time zone, and daylight saving time setting (if applicable) on a Mac is very important. File creation and modification dates use the system time. Log entries use the system time. Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes, which can affect Apple’s single sign-on feature, Active Directory logons, and other features.
Caveats: If port 123 (the NTP port) is blocked by a firewall, the automatic date and time feature will not work. If the port is blocked, a time server accessible behind the firewall must be used to set the date and time automatically. A mix of internal and external time servers is recommended for mobile systems.
Remediation: In System Preferences: Date & Time, Select the Time Zone tab. Make sure the correct Time Zone is selected. Next, select the Date & Time tab. Make sure the “Set date & time automatically” checkbox is checked. If your organization runs its own time server, enter its name in the field. You can enter multiple time servers by separating them with a space, listing them in order of preference.
Alternatively, perform the following:
Using sudo, edit /private/etc/hostconfig and change the TIMESYNC entry to -
YES-
Using sudo, edit /private/etc/ntp.conf and enter desired servers. For example:

```
server time.internal.companyname.com preferred
server time.apple.com
```

Then restart the time daemon:

```
sudo launchctl load -w \
/System/Library/LaunchDaemons/org.ntp.ntpd.plist
```

Audit

In System Preferences: Date & Time select the Date & Time tab. Make sure the “Set date & time automatically” checkbox is checked.

Alternatively, run the following commands:

```
cat /etc/hostconfig | grep TIMESYNC
```

Make sure the results are:

```
TIMESYNC=-YES-
```

```
cat /etc/ntp.conf
```

Make sure the results list desired time servers. For example: server time.apple.com

Verify the /System/Library/LaunchDaemons/org.ntp.ntpd.plist job is running

```
cat
/System/Library/LaunchDaemons/org.ntp.ntpd.plist | grep
Disabled
```

make sure the results are blank.

Additional Info

```
man ntp.conf
```

http://support.ntp.org/bin/view/Main/WebHome

By default, a system set up with the Mac OS X Setup Assistant will use one of Apple’s time servers.

Be sure you understand the ramifications if you do not use fully-qualified domain names (FQDN) or IP addresses when specifying your time servers.

Scoring Status: Scorable

Desktop & Screen Saver Preferences

Set a short inactivity interval for the screen saver

By obscuring the screen with a picture, graphic, or just an opaque color, the screen saver can keep prying eyes off of an unattended screen and potentially sensitive information.

Remediation: In System Preferences: Desktop & Screen Saver, Screen Saver Tab, make sure the Start screen saver slider is to a reasonably low value.

Alternatively, run the following command:

```
defaults -currentHost \
write com.apple.screensaver idleTime -int 900
```

where 900 is the number of idle seconds until the screen saver starts. A logout of the user may be required for the new settings to take effect.

Audit: Open System Preferences: Desktop & Screen Saver, Screen Saver Tab, make sure the Start screen saver slider is to a reasonably low value (like 15 minutes).
Alternatively, run the following command:
`defaults -currentHost read com.apple.screensaver idleTime` and verify the setting is adequately low (<= 900)

Scoring Status: Scorable

Disable users or admins to login to another users active and locked session

Administrators with rights to manage the device do not necessarily have rights to access everything the user of the computer has rights to including email, web applications and mounted shares and disk images and there are definitely privacy and personal information implications by allowing everyone with administrative rights access to any users active session

Caveats: While Fast user switching is a workaround for some lab environments especially where there is even less of an expectation of privacy this setting change may impact some maintenance workflows
Remediation: Edit /etc/authorization system.login.screensaver setting to the following:

```
<key>system.login.screensaver</key> <dict>
screensaver.</string>
<key>class</key>
<string>rule</string>
<key>comment</key>
<string>The owner can unlock the
<key>rule</key> <string>authenticate-session-owner</string>
```

Audit: `grep -ir "<string>authenticate-session-owner-or-admin</string>" /etc/authorization`
No results will be returned if the system is configured as recommended.

Scoring Status: Scorable

Energy Saver Preferences

Verify Display Sleep is set to a value larger than the Screen Saver

If the Screen Saver is used to lock the screen, verify the Display Sleep settings are longer than the Screen Saver setting. If the display goes to sleep before the screen saver activates, the computer will appear to be off, but will be unprotected.
Remediation: In System Preferences: Energy Saver, drag the slider for “Put the display(s) to sleep...” to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.
Alternatively, use the following command:

```
sudo pmset -c displaysleep 0
```

Note: The –c flag means “wall power.” Different settings must be used for other power sources.
Audit: In System Preferences: Energy Saver, verify the slider for “Put the display(s) to sleep...” to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.
Alternatively, use the following command:

```
pmset -g | grep displaysleep
```

and verify the value returned is longer than the Screen Saver, if the Screen Saver is used to lock the screen.
Additional Info
man pmset

Scoring Status: Scorable

Set a screen corner to Start Screen Saver

By obscuring the screen with a picture, graphic, or just an opaque color, the screen saver can keep prying eyes off of an unattended screen and potentially sensitive information.

Audit: The corrected audit commands for these settings are:

```
    defaults read com.apple.dock wvous-bl-corner
    defaults read com.apple.dock wvous-br-corner
    defaults read com.apple.dock wvous-tl-corner
    defaults read com.apple.dock wvous-rl-corner
```

… at least one of the above commands should return “5”.

Scoring Status: Scorable

Do not set any screen corner to Sleep Display

When this feature is used the screen goes blank but moving the mouse or pressing a button brings up the screen again with no password required. The screen saver (with its lock) will still kick in after X minutes, but the user could be lulled into a false sense of security if she sees her screen is blank and the screen saver has not activated.

Remediation: In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to Sleep Display.
The screen corners can be set using the defaults command, but the permutations of combinations are many. The plist file to check is ~/Library/Preferences/com.apple.dock and the keys are
wvous-bl-corner
wvous-br-corner

wvous-tl-corner
wvous-tr-corner
There are also modifier keys to check and various values for each of these keys. A value of 10 for any of corners should not be allowed (10 = sleep display). If any value is 10, change the value to 1 (which means no action). Also change the corresponding wvous-xx-modifier key to 1048576.
Audit
In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to Sleep Display.
Audit: The corrected audit commands for these settings are:

```
defaults read com.apple.dock | grep –i corner
```

… verify none of the *-corner keys has a value of ”10”.

Scoring Status: Scorable

Keyboard & Mouse

Disable "Allow Bluetooth devices to wake this computer"

Unless you are using a Bluetooth keyboard or mouse in a secure environment, there is no reason to allow Bluetooth devices to wake the computer. An attacker could use a Bluetooth device to wake a computer and then attempt to gain access.
Caveats: This setting is only available in the Mac is equipped with Bluetooth.
Remediation: In System Preferences: Keyboard & Mouse, Bluetooth tab, make sure the "Allow Bluetooth devices to wake this computer" is not checked.
Alternatively, run the following command:

```
defaults write /Library/Preferences/com.apple.Bluetooth \
BluetoothAutoSeekKeyboard -boolean yes
```

Audit: In System Preferences: Bluetooth, Advanced, make sure the "Allow Bluetooth devices to wake this computer" is not checked.

Alternatively, run the following command:

```
defaults read /Library/Preferences/com.apple.Bluetooth \
BluetoothAutoSeekKeyboard
```

… and verify the result is "0".

Scoring Status: Scorable

iCloud Preferences

All systems using iCloud services should be provided to the end user with the initial configuration specified below. In cases where the end user has the ability to alter the iCloud settings once the system is being used, the Service Provider has no responsibility to continuously enforce these settings. IT Service Providers may choose to include this document, or references to online copies of this document, as part of the materials provided to end users when delivering OS X devices, which include iCloud service capabilities.

Background: Apple has included a new data sharing service called iCloud with the release of Mac OS X 10.7.2 (Lion, and later versions) for Macintosh computers. iCloud provides consumers the means to sync and share electronic mail, documents, calendar reminders, browser bookmarks, contacts, and photos, by caching this data on Apple servers on the Internet and then syncing all devices associated with an Apple iTunes account. In addition, remote desktop “Back to My Mac” and geo-locator “Find My Device” capabilities have been included. As the integration point for this data sharing is the user’s personal iTunes store account. The iCloud features must be controlled on all OS X systems to prevent the exfiltration of Enterprise data onto personally owned devices or commercial Apple iCloud servers.

Specific Configuration Guidance: The following iCloud services have the listed data exfiltration capabilities and/or security concerns. If the service is enabled the following issues should be considered:

- Mail & Notes: Internal electronic mail information would be cached on Apple iCloud servers and synchronized to personal devices which share the same iTunes account. Mail & Notes should only be backed up to iCloud in an Enterprise environment where the sensitivity of that data has been deemed appropriate to back-up to Apple.
- Documents & Data: Internal documents, research, operations information, and pre-decisional analyses would be cached on Apple iCloud servers.
- iCloud Backup: Any data which is stored on a system would be stored on Apple iCloud servers, under the control of personal iTunes accounts.
- Calendars & Reminders: Normal meeting invitations include dial-in, access code, and online meeting information. The caching of internal meeting information on iCloud servers exposes this data to compromise and may allow access to meetings, attendee lists, or associated documents though download via Online meeting clients. Reminders, are a form of task-based Calendar, and as of OS X 10.8, has become a separate OS X application mimicking the iOS Reminder App. Reminders are included as a data exfiltration concern, though the task calendar may contain little data worthy of protection itself; disabling of iCloud Calendar

sharing (to protect meeting information) on OS X Lion 10.7 (or later) requires the disabling of iCloud syncing of iOS Reminders as well.

- Contacts: While much of the information included in contact data may be public information, the disclosure of internal notification or operational contacts may potentially occur. Most Enterprise email systems provide internal Contacts management and synchronization, it is recommended that this data not be synced with all personal iOS and/or OS X Lion (or later) systems that share the same iTunes account through iCloud, using the Enterprise email systems account services to provide this data to only the intended set of Apple devices.
- Back to My Mac: While not directly a data synchronization utility, the remote login utility should be disabled on OS X Lion 10.7 (and later) devices unless specifically supported by the local organization.

iCloud Services: Personnel using or supporting iOS or OS X 10.7 (and later) devices are required to disable all iCloud services with the exception of the following:

- Bookmarks
- Photo Stream (with provisos that appear below)
- Find My iPhone (or Mac)

The rationales and provisos for allowing the above services are as follows:

- Bookmarks (renamed "Safari" in later OS versions): Sensitive data and web applications are secured by the SSL protocol and require authentication. The URLs themselves are not considered sensitive.
- Photo Stream: The use of the iOS device camera for business purposes is likely to be unplanned and incidental; personnel with defined photographic roles and needs will tend to use dedicated camera equipment. The occasional business photography for participation in social networking or blog updates will occur under already established and (in most environments) posted rules for the taking of photographs. The most frequent use of the iOS device camera on enterprise equipment is likely to occur under the category of "acceptable personal use" – taking photos of personal events, as a result of the carrying of the device for mobile access to email or telephone communications. With Photo Stream activated, it should be noted that these personal photographs will automatically be synced to enterprise computer systems that have iCloud Photo Stream enabled using the same iTunes account. Users should be cautioned to be aware of this synchronization, to both ensure that business photos are not shared when they are sensitive, and that personal photographs which violate policies for acceptable data on Enterprise devices (photos that are: sexually explicit,

promote political viewpoints or candidates, are used in personal business ventures, etc.), are not synced by Photo Stream. In all cases, the use of the iOS device is already constrained by these same “acceptable personal use” policies, regardless of the source of the data, and the camera or Photo Stream is just another facet of possession of the overall device. Care should nonetheless be taken about the somewhat unique potential for personal data to infiltrate enterprise systems, since this represents a reversal of the more common concerns and controls on the exfiltration of data. *Added for iOS 6:* Photo Streams have added sharing capabilities to other iOS users, and the general public. Sharing to individuals is based on the email address used for their Apple iTunes account. Similar cautions as noted above apply to sharing photos via this method. Manual copying of photos is needed to a shared stream, in order for the photos to be shared; no default sharing of all photos seems possible. iOS device users should exercise due care in sharing photos via Photo Stream, particularly when doing so via a Public share, and/or with geo-location data enabled on photos.

- Find My iPhone (or Mac): This service may assist in the recovery of a lost or stolen device, and should be available for most users to enable. Users with concerns about the advertising of geo-location data should have the ability to disable this iCloud service on their device.

Network Preferences

Print & Fax Preferences

Only use known printers

The Mac’s ability to browse and find printers is very good. One should only print to a known printer. When at a public location, such as a hotel or trade show, many printers may appear available in the Print & Fax panel. Only print to a known printer.
Remediation: This rule cannot be implemented technically. One just has to use one’s judgment when printing.

QuickTime Preferences

Do not install third-party QuickTime software

Do not install any QuickTime software unless the source is known and trusted.

Remediation: Check that software in /Library/QuickTime and ~/Library/QuickTime is valid.
Audit: Check that software in /Library/QuickTime and ~/Library/QuickTime is valid.

Disable "Play Movies automatically"

QuickTime is used in browsers to play audio and video content. When the browser sees such content the browser passes off control to QuickTime through
its Web browser plug-in. QuickTime can be set to start playing this content immediately. Some content may contain malicious code embedded in the audio or video. Ensure the

user wants to play the embedded content by turning off the “Play Movie Automatically” option.

Caveats: The user will need to press a play button to play the content in the browser.
Remediation: In System Preferences: QuickTime: Browser tab, disable “Play movies automatically”
Audit
In System Preferences: QuickTime: Browser tab, verify “Play movies automatically” is disabled.

Security Preferences

Require a password to wake the computer from sleep or screen saver

Sometimes referred to as a “screen lock” this option will keep the casual user away from your Mac when the screen saver has started.

Remediation: The use of the –currentHost parameter no longer seems to work on 10.8. Use this instead:

```
defaults write \
com.apple.screensaver askForPassword -int 1
```

Audit: The use of the –currentHost parameter no longer seems to work on 10.7. Use this instead:

```
defaults read com.apple.screensaver askForPassword
```

… verify that the setting is ” 1”.

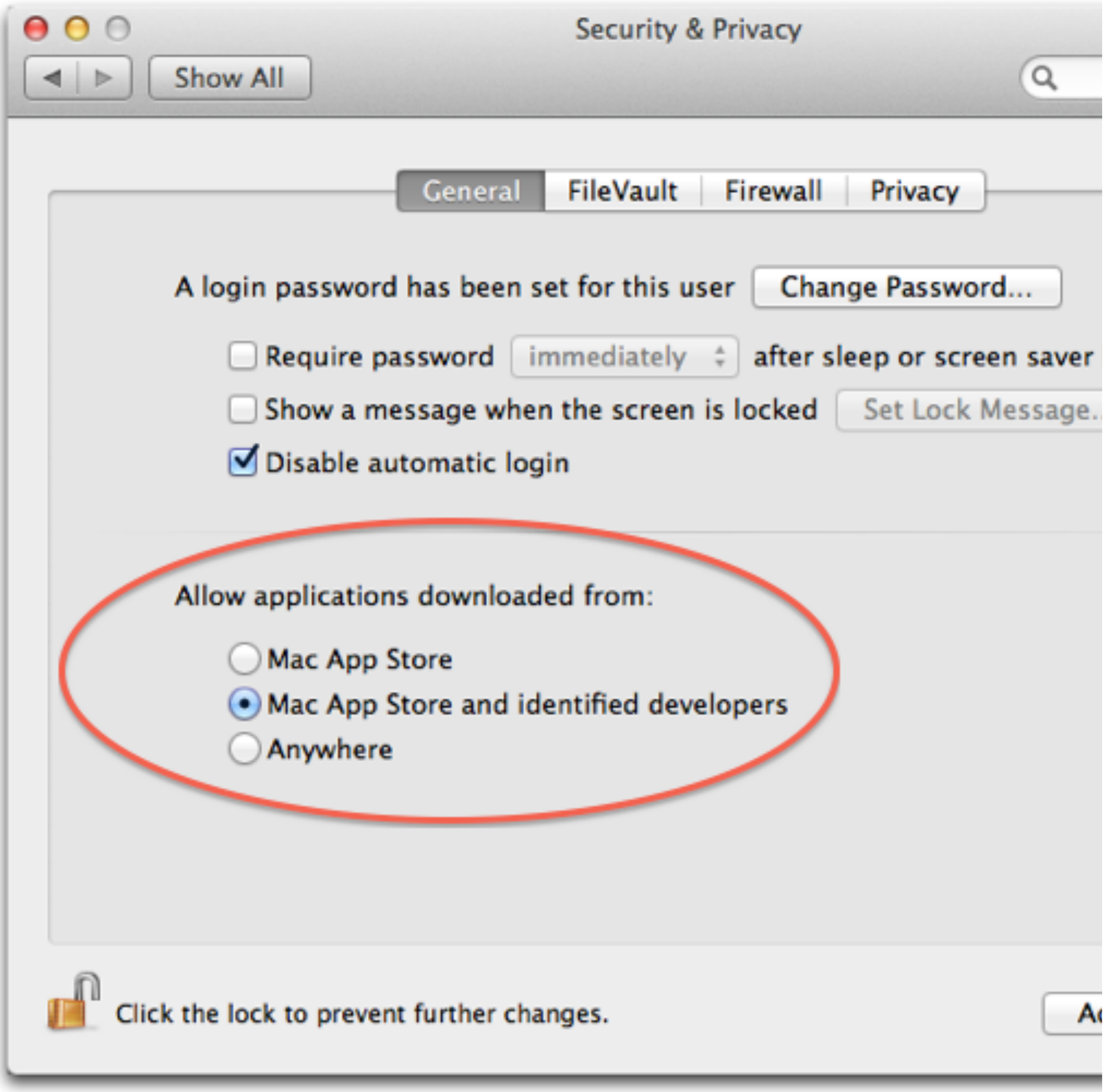
Additional Info
This only protects the system when the screen saver is running.

Scoring Status: Scorable

Gatekeeper: Signed Applications

As introduced in OS X 10.7, the Gatekeeper feature protects Macintosh systems from malware and applications from anonymous sources. Details on the feature are available in this Apple Support article.

Gatekeeper preferences for systems should be set to “Allow applications downloaded from: Mac App Store and identified developers”, as depicted in the circled section of this screenshot:



A login password has been set for this user

□ Require password immediately after sleep or screen saver

□ Show a message when the screen is locked

☑ Disable automatic login

Allow applications downloaded from:

○ Mac App Store

● Mac App Store and identified developers

○ Anywhere

Click the lock to prevent further changes.

IT service providers or system owners selecting the “Anywhere” option for Gatekeeper configuration should address the added vulnerability and any mitigation actions in the IT Security Plan for the target system(s).

Context: System

Scoring Status: Not Scorable
Audit: In System Preferences: Security, General tab, verify “Mac App Store and identified developers” is checked.

Automatically update safe downloads list

Files downloaded via applications such as Safari, iChat, and Mail are checked for safety at the time that they are opened. If a file is identified as containing known malware, the system will display a dialog that alerts you to move it to the Trash. You should empty the Trash to finalize the removal of the file. Apple maintains a list of known malicious software that is used during the safe download check to determine if a file contains malicious software, the list is updated dCaveats: Apple will push updates to the computer for malware definition files
Remediation: In System Preferences: Security & Privacy, Advanced tab, ensure that “Automatically update safe downloads list” is checked
Additional Info: https://support.apple.com/kb/HT4651

Disable “automatic logout” after a period of inactivity

If the machine automatically logs out, unsaved work might be lost. The same level of security is available by using a Screen Saver and the “Require a password to wake the computer from sleep or screen saver” option.

Caveats: This option might be appropriate for kiosk Macs or for other organizational reasons.
Remediation: In System Preferences: Security & Privacy, Advanced tab, uncheck “Log out after X minutes of inactivity.”
Alternatively, run the following command

```
sudo defaults write \
/Library/Preferences/.GlobalPreferences \
com.apple.autologout.AutoLogOutDelay -int 0
```

Audit: In System Preferences: Security, General tab, verify “Log out after X minutes of inactivity” is unchecked.
Alternatively, run the following command

```
defaults read /Library/Preferences/.GlobalPreferences \
com.apple.autologout.AutoLogOutDelay
```

and verify the result is 0.

Scoring Status: Scorable

Enable FileVault

FileVault offers protection for data at rest. This means that the data is only protected when the user is not logged in, which is useful if the computer is stolen.

Caveats: There are many caveats to using FileVault. Apple does not provide a means for organizational key recovery if the password is lost. Double the size of the user’s home directory is required to be available on the hard drive when FileVault for the user is turned on. Not everything on the disk is encrypted, so a false sense of security may ensue when using FileVault. And finally, FileVault can cause a significant slowdown of the system. All that said, however, FileVault is still a good method to provide data at rest protection.

There are also challenges in using FileVault with Directory accounts, particularly around external password changes and password expiration on off-line computers.

Note: Encrypting user data is not foolproof. Proof of concept attacks by security researchers have recently shown that computer memory, even in a Mac, is readable for up to ten minutes after shut down! When shutting down a Mac, make sure the computer is protected from physical access for at least ten minutes.

Remediation: The use of FileVault has moved to Level 1. The detailed information on its use is discussed later in this document.
Audit: Audit this setting by confirming that FileVault is enabled and a Master Key is set in the System Preferences.

With the arrival of OS X 10.7, FileVault version 2, full disk encryption was added. While many of the same caveats (as discussed in the CIS OS X 10.6 Benchmark) regarding software encryption and organizational key escrow remain with FileVault version 2, the use of this software is now required for all Macintosh end user systems beginning with OS X 10.7 (and subsequent versions of OS X.) FileVault keys should be escrowed with Apple when there is no organizational means to escrow these keys with the system service provider. While there is some potential of data loss for individual end user systems with FileVault enabled, this risk is deemed less critical than the continued known exposure of organizational data on unencrypted end user systems.

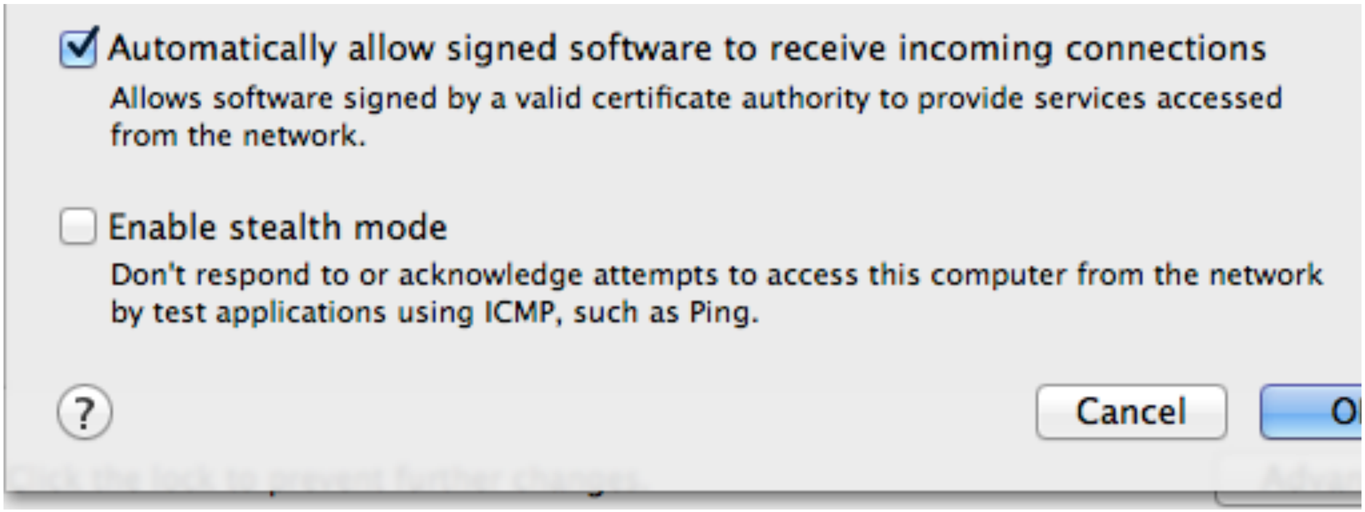
Scoring Status: Scorable

Enable firewall protection

Apple's firewall will protect your computer from certain incoming attacks. Apple offers three firewall options: Allow all, Allow only essential, and Allow access for specific incoming connections. Unless you have a specific need to allow incoming connection (for services such as SSH, file sharing, or web services), set the firewall to "Allow only essential services," otherwise use the "Allow access for specific incoming connections" option. Only enable stealth mode if approved by your network engineering, scanning or security team.

Remediation: In System Preferences: Security, Firewall set "Turn On Firewall"

Firewall Options set “Automatically allow signed software to receive incoming connections”.



☑ Automatically allow signed software to receive incoming connections

Allows software signed by a valid certificate authority to provide services accessed from the network.

□ Enable stealth mode

Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

<u>**Configure “Enable Location Services”**</u>

Apple’s Privacy settings allows for control over whether or not Applications have access to the system’s location.
Context: System
Scoring Status: Not Scorable
Remediation: In System Preferences, Security and Privacy, Privacy tab, uncheck “Enable Location Services”. If it is necessary to “Enable Location Services” enable only specific applications.

<u>**Configure “Access to Contacts”**</u>

Apple’s Privacy settings allows for control over whether or not Applications have access to Contacts. In Systems Preferences, Security and Privacy, Privacy tab, uncheck specific Applications to disallow access to Contacts.
Context: System
Scoring Status: Not Scorable
Remediation: If it is necessary allow only specific applications access to Contacts.

Sharing Preferences

<u>**Configure Screen Sharing**</u>

Screen Sharing uses the open source VNC protocol to let one computer observe or control the screen on another computer. Apple Screen Sharing is encrypted (using a proprietary encryption protocol), so others cannot eavesdrop on a screen sharing session. The most important aspect of securing screen sharing is to make sure only the correct people can observe or control the Mac.
Apple allows for a few options when configuring screen sharing and each has its place for a secure Mac. These option are not mutually exclusive.
1. Screen Sharing off

This is the most secure option.
2. Anyone may request permission to control screen
This is the second most secure option. When a remote user attempts to share the screen, the Mac will prompt the local user for permission. If the local user doesn't grant permission, the remote user cannot share the screen. If a local
user is not at the Mac to grant permission, then the screen cannot be shared.
3. VNC viewers may control screen with password
This is the least secure option since the remote user only needs to know the password.
4. Allow access to all users of the Mac, or specific users (or groups of users)
Allowing access to only users with accounts on the Mac, or if a directory service (like Open Directory or Active Directory) is used, specific users or groups, allows some restriction of who can share the screen. Any authorized user would be able to observe or control the screen without the express permission of the local user. This option should only be used when necessary (possibly in a school environment).

Caveats: A thorough understanding of each setting's advantages and disadvantages is necessary when turning Screen Sharing on.
Remediation: In System Preferences: Sharing, turn on Screen Sharing only if necessary. Configure Screen Sharing according to personal or organizational needs, but be aware of the implications of each option.

Screen Sharing

Apple's screen sharing functionality with OS X 10.7 approaches the level of Microsoft Remote Desktop Services, allowing a second user to remotely access an independent graphical system session. The mechanism used is the Virtual Network Computing (VNC) protocol, requiring firewall adjustments for inbound session connections. Users are granted access via their Apple IDs, or normal user account names and passwords. The default System Preferences for Screen Sharing restricts the capability to only administrator user accounts, unless others are added. Given the same functionality as Microsoft Remote Desktop, similar security concerns exist (exposure on public networks, as an avenue for brute-force password guessing, etc.), along with the additional concern of users who may grant others access to their systems using Apple IDs as authentication. Apple Screen Sharing shall be disabled on all OS X systems.

Disable File Sharing

Apple's File Sharing uses a combination of many technologies: FTP, SMB (Windows sharing) and AFP (Mac sharing). Generally speaking, file sharing should be turned off and a dedicated, well-managed file server should be used to share files. If file sharing must be turned on, the user should be aware of the security implications of each option. Turning on File Sharing automatically shares the entire hard drive to anyone with an account on the Mac, or anyone who can access the Mac using a network account. File and folder access control restrictions are enforced by default, so user Mary cannot access user Joe’s Documents folder (by default). Specific access controls can be relaxed or strengthened for specific folders in the Sharing System Preference pane.

Each method of sharing files has advantages and disadvantages. Regardless of which method used, the folder and file access permissions must be controlled to make sure only the correct data is shared. The three ways to share files using File Sharing are:1

1. Apple File Protocol (AFP)

AFP under Snow Leopard automatically uses encrypted logins, so this method of sharing files is fairly secure. The entire hard disk is shared to administrator user accounts. Individual home folders are shared to their respective user accounts. Users’ “Public” folders (and the “Drop Box” folder inside) are shared to any user account that has sharing access to the computer (i.e. anyone in the “staff” group, including the guest account if it is enabled).

2. File Transfer Protocol (FTP)

FTP send password via clear text and thus is very insecure. FTP is commonly used for anonymous upload and download of files where security is of less concern. FTP should not be used on a client Mac except in rare case for temporary anonymous sharing.

3. Server Message Block (SMB), Common Internet File System (CIFS)

When Windows (or possibly Linux) computers need to access file shared on a Mac, SMB/CIFS file sharing is commonly used. Apple warns that SMB sharing stores passwords is a less secure fashion than AFP sharing and anyone with system access can gain access to the password for that account. When sharing with SMB, each user that will access the Mac must have SMB enabled.

Additional Information: Technically the Mac can share files other ways out of the box: Secure Copy Protocol (scp), secure File Transfer Protocol (sftp), and Network File System (NFS). scp and sftp are a subset of the Remote Login feature and are discussed is the Remote Login section of this document. Apple doesn’t provide a GUI means of enabling NFS, so the NFS protocol will not be discussed in this document. NFS poses significant security risks and should only be configured by an experienced system administrator familiar with inherent NFS risks.

Caveats: A thorough understanding of each protocol’s advantages and disadvantages, as well as an understanding of what folders and files are shared is necessary when turning File Sharing on.

Remediation: In System Preferences: Sharing, turn on Screen Sharing only if necessary. Configure Screen Sharing according to personal or organizational needs, but be aware of the implications of each option.

To turn off AFP from the command line:

```
sudo launchctl unload -w \
/System/Library/LaunchDaemons/com.apple.AppleFileServer.pli
st
```

To turn off FTP from the command line:

```
sudo launchctl unload -w \
/System/Library/LaunchDaemons/ftp.plist
```

To turn off SMB sharing from the CLI:

```
sudo defaults delete \
/Library/Preferences/SystemConfiguration/com.apple.smb.serv
er \ EnabledServices
sudo launchctl unload -w \
System/Library/LaunchDaemons/nmbd.plist
sudo launchctl unload -w \
/System/Library/LaunchDaemons/smbd.plist
```

Audit: In System Preferences; Sharing, File Sharing; Options, verify only the needed sharing services are on.

Alternatively, run the following commands:

```
launchctl list
```

and look for the various services listed above in the remediation section.

Additional Info: If authenticated ftp is used all console and SSH users should be entered into the /etc/ftpusers list to deny ftp access for those users with full access.

Scoring Status: Scorable

__Turn off Printer Sharing__

Printer Sharing makes the Mac into a print server. Attackers could attempt to exploit the print server to gain access to the Mac. As with File Sharing, Printer Sharing is best left off and a dedicated, well-managed print server or a printer with built-in IP network capability is recommended.

Remediation: In System Preferences: Sharing, turn off Printer Sharing.

Audit: In System Preferences: Sharing, verify Printer Sharing is off for each printer listed.

__Turn off Scanner Sharing__

Context: System

Scoring Status: Not Scorable

Remediation: In System Preferences: Sharing, turn off Scanner Sharing.

Audit: In System Preferences: Sharing, verify Scanner Sharing is off for each printer listed.

__Configure Remote Management__

Remote Management is the client portion of Apple Remote Desktop (ARD) < http://www.apple.com/remotedesktop/>. Remote Management has a screen sharing component similar to the Screen Sharing feature described above. Remote Management can also be used by administrators to install software, report on, and generally manage client Macs. ARD is mostly likely to be used in an organization and not by home users.

The screen sharing options in Remote Management are identical to those in the Screen Sharing section. In fact, only one of the two can be configured. If Remote Management is used, refer to the Screen Sharing section above on issues regard screen sharing.
Other features of Remote Management should be configured if the service is used. One option is to “Show Remote Management status in the menu bar.” Turning this option on allows the user to see if screen sharing or other remote management features are being used.
More security settings of relevance are found after clicking on the Options button. Only those options needed by the Remote Management Administrator should be turned on.
The final security concern with Remote Management is the list of users that access the Mac with Remote Management. The easiest and least secure method, is to have the same username and password for a Remote Management administrator on every Mac in an organization. If this one name/password combination is compromised, the entire network of Macs is compromised.
The second method would be to have a different username/password combination on each Mac. This is difficult to implement since one would need to remember a large number of passwords and usernames, or one would need to write them down, thus creating a target for compromise.
The ideal solution is to use a directory service (like Open Directory or Active Directory) and only allow group access. This method allows an organization to add or remove people to the directory group as needed, thus controlling access to the network of Macs. There are four groups used by ARD for this purpose: ard_admin, ard_interact, ard_manage and ard_reports. Therefore, combining or nesting local or network groups and user accounts may meet your needs. Various versions of Mac OS X and ARD may or may not allow the use of these groups, particularly if groups are nested within groups.

Caveats: A wide variety of configuration permutations are possible with Remote Management. Remote Management should be configured by an experienced administrator.
Remediation: In System Preferences: Sharing, turn on Remote Management if necessary. If turned on, configure the screen sharing options as discussed above in the Screen Sharing section. Turn on the option: “Show Remote Management status in the menu bar”
Only turn on the options in the Options button if necessary.
Use a directory service to allow Remote Management access. Do not use a common username/password across multiple Macs.
Audit
Use the kickstart program to set or determine Remote Management settings.
Additional Info

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/
Contents/Resources/kickstart -helpDisable Remote Apple
Events
```

Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer. Typically Remote Apple Events is used to automate a business process. Unless needed, Remote Apple Events should be turned off. If needed, it should be configured with the least access granted as possible. If Mac OS 9 is not being used, the option to allow events from OS 9 should be turned off. If OS 9 events are needed, a username and password should be used.

Context: System
Scoring Status: Scorable
Remediation: In System Preferences: Sharing, turn on Remote Apple Events only if necessary. If turned on, add users to the Allow Access for list if possible
To turn off Remote Apple Events from the command line:

```
sudo launchctl unload -w \
/System/Library/LaunchDaemons/eppc.plist
```

Audit: In System Preferences: Sharing, verify Remote Apple Events is off. Alternatively, run the following command:

```
launchctl list | grep –I eppc
```

There should be no results.

Disable Internet Sharing

Internet Sharing uses the open source natd process to share an internet connection with other computers and devices on a local network. Unless specifically required, Internet Sharing should be turned off. If used, it should only be turned on when actual sharing is needed. A much better solution is a dedicated router (available for as little as $10US). Apple makes a number of certified compatible routers.
Remediation: In System Preferences: Sharing, turn on Internet Sharing only if necessary. Alternatively, run the following commands:

```
sudo defaults write \
/Library/Preferences/SystemConfiguration/com.apple.nat \
NAT -dict Enabled -int 0
sudo launchctl unload -w \
/System/Library/LaunchDaemons/com.apple.InternetSharing.pli
st
```

Audit
In System Preferences: Sharing, verify Internet Sharing is off. Alternatively, run the following commands:
Additional Info: http://www.apple.com/wifi/

Turn off Bluetooth Sharing

Context: System
Scoring Status: Not Scorable
Remediation: In System Preferences: Sharing, turn off Bluetooth Sharing.
Audit: In System Preferences: Sharing, verify Bluetooth Sharing is Off .

Software Update Preferences

Disable “Check for updates” for standard users

Since most updates require an administrative password to install, there is little need to notify standard users when updates are available. The exception would be if the standard user also has an administrator account on the same Mac.

Caveats: Only disable for standard users that do not have an administrator account.
Remediation: In System Preferences: Software Update, turn on “Check for updates” for administrator accounts, and for standard users that also have an administrator account. Turn off “Check for updates” for all others.Sound Preferences

Dictation & Speech Preferences

Only enable speech recognition in a secure environment

Apple’s speech recognition allows a user to speak a finite list of commands that are recognizable by the computer. If configured improperly, anyone within earshot of the Mac can initiate these actions. Use of speech recognition should be in a secure environment where Remediation: In System Preferences, Speech, Speech Recognition tab, turn off Speakable Items unless in a secure environment.
Audit: In System Preferences, Speech, Speech Recognition tab, verify Speakable Items is off.
Additional Info: Apple’s speech recognition is listener independent, does not require training, and is optimized for a speaker within about 21 inches of the built-in microphones on Macintosh models. It may work better with a speech-quality microphone. A brief calibration routine for each user (and often, in each new aural environment) is recommended.
The speech command sets enabled by default include:
Address Book
Global Speakable Items (such as “What time is it” and “What day is it”)
Application Specific Items (provided in the bundles of running applications)
Application Switching.
Additional Speakable Items are found in ~/Library/Speech/Speakable Items, a directory which does not exist by default (and is not in the User Template).

Configure Speech Recognition to use a Listening Key

Speech Recognition can be configured to listen continuously or only when a specific key is pressed. Listening continuously can allow anyone within earshot of the Mac to initiate an operation on the Mac. Configure speech recognition to use a Listening Key to commands are

Remediation: In System Preferences, Speech, Speech Recognition tab, select “Listen only while key is pressed”.

Audit: In System Preferences, Speech, Speech Recognition tab, verify “Listen only while key is pressed” is selected.

Use headphones if you enable text to speech, or turn text to speech off

When using the Text to Speech feature, use headphones to others cannot hear what the computer is saying. The computer may convert sensitive text to speech, so limit who can hear it.
Remediation: In System Preferences, Speech, Text to Speech tab, turn off all options or wear headphones.

Spotlight Preferences

Prevent Spotlight from searching all confidential folders

Spotlight is Apple’s search technology built into the operating system. By default it indexes every file on any local hard drive. While spotlight will enforce access control restrictions to limit access to files, the index itself may contain information about sensitive files that others should not see. The Spotlight System Preference Pane allows the user to exclude volume, folders, and data types from being indexed.

Caveats: Adding folders or volumes to the privacy settings will restrict searching for information in those folders and volumes. For example, adding ~/Library/Mail will disable the ability to search through the body of Mail messages, even within the Mail application.
Also, authentication is not required to add or remove items to the exclusion list. Any user can remove items from the exclusion list.
Remediation
In System Preferences: Spotlight, Search Results tab turn off any categories that should not be indexed.
In System Preferences: Spotlight, Privacy tab add any volumes or folders that contain sensitive data.
Alternatively you can disable spotlight from indexing and search specific volumes with the following command:

```
sudo mdutil -E -i off <volumename>
```

Prevent Spotlight from searching backup folders or volumes

Spotlight is Apple’s search technology built into the operating system. By default it indexes every file on any local hard drive. If a local hard drive is used for backup, spotlight will find the original and the backup of a file. The user may edit the backup file and lose changes if the back up file overwrites the backup with the original.

Remediation: In System Preferences: Spotlight, Privacy tab add any volumes or folders that contain backups.
Audit: In System Preferences: Spotlight, Privacy tab verify all backup volumes or folders are in the privacy list.

Time Machine Preferences

Time Machine

Backing up is very important. This point cannot be stressed enough. Apple includes Time Machine to make backing up easier. Numerous third party free and commercial products are also available to back up one's Mac. A good backup scheme can mitigate the loss of data if a Mac is compromised, lost, stolen, or becomes unusable.

Remediation: When using Time Machine, simply connect and external drive to the Mac and the Mac will ask if you want to use the drive as a backup drive. Select yes.
When using other software, follow the software's instructions to backup.

Securely erase files in the Finder

When a file is put into the trash and trash is emptied, only the directory entry for the file is deleted; the data in the file is not actually deleted.
Think of a magic book library. When the librarian wants to remove a book she just removes the card catalog card for the book. The book stays on the shelf until the space is needed. When space is needed, pages from the book are removed until the needed space is made available. Until all the space of the original book is needed, some pages may remain on the shelf.
The computer operates in a similar fashion. The data from the file is still on the hard drive until the operating systems needs the space. "Undelete" software is available to recover these files, and special disk reading software is available to look at partial remains of the file if part of its space is used.
To be sure a deleted file is actually deleted, the Mac has a feature called Secure Empty Trash (under the Finder menu). When selected the Mac not only removes the file information from the file directory, the Mac also overwrites the data in the file with meaningless data, thus preventing the file from being recovered.
Use Secure Erase Trash to erase sensitive files.
Finder: Preferences: Advanced allows the user to set Empty Trash Securely as the default.
The command line tool `srm` is also available as an alternative to `rm`.

Caveats: Secure Empty Trash can take a long time. If the user's home folder is using FileVault that extra time is being taken to erase part of an encrypted file.
Remediation: When emptying the trash, use Finder: Secure Empty Trash if sensitive files are in the trash.
If sensitive files are commonly deleted, set the Finder: Preferences: Advanced Empty Trash Securely option to on.
Use the srm command in Terminal when deleting sensitive files from the CLI.
Additional Info: `man srm`

Remediation

Safari should not open safe files after downloading

Safari will automatically run or execute what it considers safe files. This can include installers and other files that execute on the operating system. Malware has taken advantage of this

Caveats: User will have to manually open files from the downloads folder
Remediation:
1. Start the Safari program.
2. Select Preferences from the Safari menu on the left side of the menu bar. 3. Choose the "General" tab.
4. Uncheck the box that says "Open 'safe' files after downloading". Quit Safari.

Mac App Store

The Macintosh App Store was present in OS X 10.6 and becomes further emphasized in OS X 10.7 and OS X 10.8 as the primary route for the installation of applications and even operating systems. While the installation of software continues to require administrative rights, the convenience of having administrative privileges on OS X systems continues to increase as well. Apple's management and cryptographic signing of App Store software reduces (if not eliminates) concerns about software including viruses, trojans, or other malware. Apple systems which are self-administered and have upgraded to Lion from Snow Leopard have likely done so through an App Store purchased and downloaded version of the 10.7 operating system. The Apple Xcode utilities required to compile executable code at the command line, manage software projects in a GUI interface, and build iOS applications, are now provided through App Store download. Since purchase and installations rights are based on an end user's Apple ID, software procured for personally-owned Macintosh systems are available for installation to Enterprise OS X systems. Productivity software such as Evernote, password keeper programs like 1Password, and utilities like CCleaner, are useful in both personal and work environments. While there are no specific security controls which result from this added feature, service providers should be aware that there is likely to be an increase in the number of self-installed personal productivity applications on Enterprise systems. Service providers should ensure that updating and patching services for App Store applications are allowed to continue to operate as Apple intended as part of the Macintosh system service delivery, so that App Store applications may be appropriately maintained on end user systems.

AirDrop

AirDrop is a wireless peer-to-peer file sharing and transfer mechanism with automatic discovery of peers in the local physical area. Files are encrypted during transfer with TLS and firewall rules are temporarily adapted to restrict access to only the systems that are exchanging files. AirDrop functions and a system's visibility are only active while the AirDrop window is open. The identify of the users transferring files are verified through their Apple ID, if the users are signed in. In operation, AirDrop is a convenience feature, similar to the use of a USB drive for the impromptu transfer of files between consenting users. Given the limited distance, temporary enablement, encrypted transfer capability, ability to identify the end points and constraint of network access to those end points, AirDrop is deemed acceptable for the transfer of non-sensitive files and data between systems.

Facetime

Apple's Facetime video conferencing software, as seen on the iPhone and iPad iOS, has arrived on the OS X systems with 10.7. By default, Facetime is disabled for each end user and must be enabled by login with the appropriate user's Apple ID at first use. Given the requirement for manual enablement and manual acceptance of Facetime "calls", as well as the general presence of video conferencing software (and hardware) on most mobile end user systems, OS X 10.7 (and later) Apple system users should have this functionality available to them. There is no requirement to disable Facetime operation on OS X, or configure this service beyond the default OS X 10.7 and above settings.

Optional Practices

Disable AirPort

There is no expectation that laptops running OS X should keep wifi turned off unless there are specific mission or travel need to do so.

If Airport is installed and not needed, disable it. There is no need to allow attackers a possible route to the Mac.

Remediation: In System Preferences: Network, select the Airport interface and click the minus button or turn the Airport card off.

Audit: In System Preferences: Network, select the Airport interface and verify the Airport card off.

Disable Bluetooth

Bluetooth is a technology which allows a wide variety of HID and other devices to be used wirelessly with a workstation, and will be commonly used with user workstations.

If Bluetooth is installed and not needed, disable it. There is no need to allow attackers a possible route to the Mac.

Remediation: In System Preferences: Network, select the Bluetooth interface and click the minus button or turn Bluetooth off.

Audit: In System Preferences: Network, select the Bluetooth interface and verify that Bluetooth is not offered as a network interface option.

Disable Bluetooth by using System Preferences for each user account

As stated earlier, Bluetooth can be very useful, but can also expose a Mac to certain risks. Unless specifically needed and configured properly, Bluetooth should be turned off

Caveats: Removes Bluetooth functionality.
Remediation: In System Preferences: Bluetooth, uncheck the “On” box. Alternatively, run the following commands:

```
sudo defaults write \
/Library/Preferences/com.apple.Bluetooth \
ControllerPowerState -int 0
sudo killall -HUP blued
```

Audit: In System Preferences: Bluetooth, verify ”On” box is unchecked. Alternatively, run the following command:

```
defaults read /Library/Preferences/com.apple.Bluetooth \
ControllerPowerState
```

and make sure the value returned is 0.