Mac OS X Configuration Guide

By Lawrence I. Charters

Note: this is intended as a *brief,* accessible guide for use by non-specialists. Apple publishes an excellent 351-page guide to Mac OS X Tiger security at:
http://images.apple.com/server/docs/Tiger_Server_Security_Config_021507.pdf

Defaults

Mac OS X installs, by default, with no externally accessible ports, functions, or services. Unless required for a specific purpose, no ports, functions or services should be enabled in Mac OS X.

Verify Drives

IDE writeable volumes should be "zero formatted" (i.e., every byte written with zeros) prior to use in order to verify that all addressable bytes on the drive are valid.

- Boot from the operating system Install 1 Disc or DVD;
- Cancel installation; select Disk Utility;
- Select the target volume;
- Select Erase tab; name the drive something other than "Macintosh HD" or your family name;
- Select Security Options;
- Select Zero Out Data (or if you have patience, 7 Pass Erase)

Disk Utility should always report the S.M.A.R.T. Status of any device as "Verified." If it reports anything else, replace the device.

Operating System Installation Process

Restore original contents

After erasing and verifying the drive, use the System CD or DVD that came with the machine to do a complete restore. This will restore all bundled software, too.

Install Mac OS X 10.4

If the restore did not install Mac OS X 10.4:

- Boot with the Mac OS X 10 .4 DVD;
- Run the install with all default options. Do not add or remove any foreign fonts (the default install set of some non-Roman fonts are required by some error traps) or printers.

Admin account

During installation, an initial administrative user name will be requested. Do *not* enter any variant of "admin" or "administrator" "or "root."

- User name: enter a one-word name you will remember, but not your name or family name or anything easily guessed ("Sweetums" is good, "Smith" is bad);
- Short name: same as user name
- Password: should be no less than eight characters, should be something you remember, and should differ from your day-to-day account name.

Working account

Once the Mac is ready for use, create a second account for day-to-day work. Use this second account for everything; the Admin account you first created should only be used for diagnostics and certain kinds of installations. In creating the second account, do not check the "Allow user to administer this computer" box.

Other choices

- Set the Time Zone to the nearest city listed in the pane;
- Set the host to use a NTP server (use the default choice);
- Do not set an IP address unless the machine is wired to a specific address on the network;

Install updates

Once installation from the install disc or discs is complete, reboot the host. Software Update should launch automatically after login. Download and install all appropriate updates. Reboot as necessary, and manually run Software Update until all appropriate updates have been installed.

Post installation configuration

Install Menu Eject

Many newer Macs lack an eject button for the CD-ROM drive. You can add an Eject control to the main menu bar.

- From the Go menu, select Go to Folder
- Type /System/Library/CoreServices/Menu Extras/
- Double-click Eject.menu; this installs an Eject button in the menu.

System Preferences

These System Preferences will enhance the speed, stability, security, and throughput of the machine.

- Desktop & Screen Saver: Set Screen Saver to Computer Name; set the Hot Corner to the lower left; set the time to no more than 15 minutes;
- Security: Check "Require password to wake this computer from sleep or screen saver;"
- Displays: check "Show displays in menu bar"
- Sound: Set Alert volume to maximum, and to show in menu bar;
- Startup Disk: Verify Startup Disk is set to the boot volume;
- Sharing: Computer Name should be set to something other than your name or nickname, and should not be "Mac" or "Macintosh;"
- Software Update: Make sure "Check for updates" is checked;
- Accounts: Set Login Options to "Name and Password," and uncheck "Show password hints"

Firewall settings

Use System Preferences to set the firewall settings using the Sharing pane. By default, all services are turned off.

- Under Firewall, select only those services necessary for your needs; normally, everything will be unchecked;
- Within the Firewall tab, select Advanced and select Enable Firewall Logging;

- Stealth Mode and Block UDP Traffic are recommended, but the latter may interfere with QuickTime broadcaster or iChat video.

Virus protection

Despite numerous false alarms, there are no Mac OS X viruses. Nonetheless, those who exchange a great many files with others (editors, photographers, teachers, graphic artists, printers, etc.) should invest in a virus checker to scan client files. Virus checkers are usually also required of government contractors.

Techie Stuff

Edit motd

Edit /etc/motd using pico. Delete the default message and replace it with anything you wish but do *not* include your name or any mention of Mac or Macintosh.

Edit ssh settings

Edit the ssh defaults to disable Level 1 ssh fallback.
- Use pico to edit /etc/sshd_config;
- Uncomment protocol fallback by changing #Protocol 2,1 to Protocol 2.

Check your work

Within the Utilities folder, launch Network Utility:
- Select the last tab, Port Scan;
- Type in the address "localhost" (without quotes);
- Press Scan.

References:

A more comprehensive security guide, five times as long (15 pages instead of three) is available from The Center for Internet Security:
"CIS Mac OS X Tiger Level I Security Benchmark, Ver. 2.0"
http://cisecurity.org/bench_osx.html