



# MAC OS X PANTHER

IN A NUTSHELL

*A Desktop Quick Reference*

O'REILLY®

*Chuck Toporek, Chris Stone  
& Jason McIntosh*



# 13

## Security Basics

---

Thanks to the inherent security of its Unix foundation and a secure-by-default configuration, Panther doesn't give its users much to worry about at first boot-up. However, Panther does include several features that help keep out intruders as you accumulate data and customize the default configuration.

Potential threats exist to many elements of an operating system, and, in most cases, Panther's security features address them to a degree greatly surpassing what's required for a typical user. With a bit of additional tightening, Panther can operate with a level of security acceptable for even much more sensitive environments.

### General Security

Panther has several general security features that contribute to the protection of the entire system.

### Unix Features

As was covered in Chapter 7, Mac OS X's Unix foundation provides for the basic permissions model that keeps system and user files and processes separate and protected. But equally important for security is Panther's open source roots, in the form of Darwin, which allows anyone to scour the source code for potential vulnerabilities and provide (or allow Apple to provide) fixes quickly. Darwin's source code, corresponding with the open source core that ships with Panther, is available freely through <http://developer.apple.com/darwin>. Apple generally makes available new Darwin versions not long after they've been released as part of each new Mac OS X version.

Also, because Mac OS X can run much of the same software available to other Unix platforms, a large amount of additional security-related software is available

for it as well. See Chapter 27 to learn more about acquiring and installing Unix software.

## Default Security

Panther is arguably the most secure of any operating system upon initial boot-up. This is mostly due to its conservative default system configuration, which ensures that your Mac will be safe from most security threats without additional configuration on your part. Here are a few things that Mac OS X Panther does by default to help make your Mac secure:

### *Disabled root account*

Typically, an intruder will attempt to access the root account to obtain complete system control, but as long as the root account stays disabled, the attempts will fail. In fact, Panther provides enough alternatives to the legitimate use of the root account that enabling it is usually not necessary even for system administrators. For example, users can instead authenticate in the Finder to access most protected areas or use *sudo* at the command line to run commands requiring root privileges.

### *Few open communication ports*

A port scan of a new Panther system will find no open TCP ports at all and only two open UDP ports. This makes for a system so secure, in fact, that turning on the firewall at this point adds no further protection (because there are no vulnerable ports that need blocking).

The two open ports are UDP 123 used by *ntpd* (the Network Time Protocol Daemon), and 5353, used by *mDNSResponder*, which is part of Rendezvous. Though there are no known vulnerabilities to either daemon, you can turn off the first by unchecking “Set Date & Time automatically” in the Date & Time preferences panel. To keep *mDNSResponder* from launching at startup and eliminate most of Rendezvous’ functionality, use the *chmod* command to turn off the executable bit of its StartupItems script, */System/Library/StartupItems/mDNSResponder/mDNSResponder*, and then restart your Mac.

### *No running network services*

With no ports open, then, you’ll also find that Panther has none of its network services turned on by default. Furthermore, only administrators can turn on these services, which include all those listed in the Sharing preferences pane.

## Software Update

Software Update helps ensure that the latest security updates, as well as the regular OS and application updates, are applied promptly. These updates, typically provided by Apple within days of a vulnerability announcement, can address one or several security issues at a time, involving both Apple software as well any of the included Unix software, such as OpenSSH or Apache. A list of all Mac OS X security updates is kept at [http://www.info.apple.com/usen/security/security\\_updates.html](http://www.info.apple.com/usen/security/security_updates.html).

Installing system software over the Internet has its own security implications, so the Software Update process uses digital signatures to protect against possible deception on the network. Each update package on Apple's Software server contains a digital signature, which when verified by your Software Update client application, guarantees that the source of the update package is indeed Apple Computer and that the package's data hasn't been modified.

## Authentication

These authentication-related security features provide additional protection for your computer while still allowing easy and secure verification for authorized users.

### Long Passwords

Panther supports account passwords of virtually unlimited length. In practice, however, you shouldn't set a password that's longer than you're willing to type (most authentication windows don't accept pasted text). Also, command-line utilities can have password length limits of their own. For example, the *sudo* utility doesn't accept passwords longer than 256 characters.

### Keychain Access

The Keychain Access application (*/Applications/Utilities*) has other security-related features in addition to its primary function as a repository for your passwords.

#### Menu extra

Keychain Access has its own menu extra, shown in Figure 13-1, which is activated by selecting View→Show Status. From the Keychain menu extra, you can lock and unlock your keychains as well as open Keychain Access and the Security preferences pane.



Figure 13-1. The Keychain menu extra

Additionally, by selecting the Lock Screen option from the Keychain menu extra, you can immediately activate a password-protected screensaver. With this option

selected, a password is required to disengage the screensaver, even if you haven't selected to always use one in the Security preferences pane (see the "Screen Locking" section of this chapter).

## Secure Notes

You can store any text you would like to keep private in a Secure Note. From Keychain Access's File menu, select New Secure Note Item, name the note and add whatever data you want encrypted and password-protected (Figure 13-2). This is a convenient way to store passwords for applications or systems that don't support the keychain, as well as credit-card numbers and PINs.

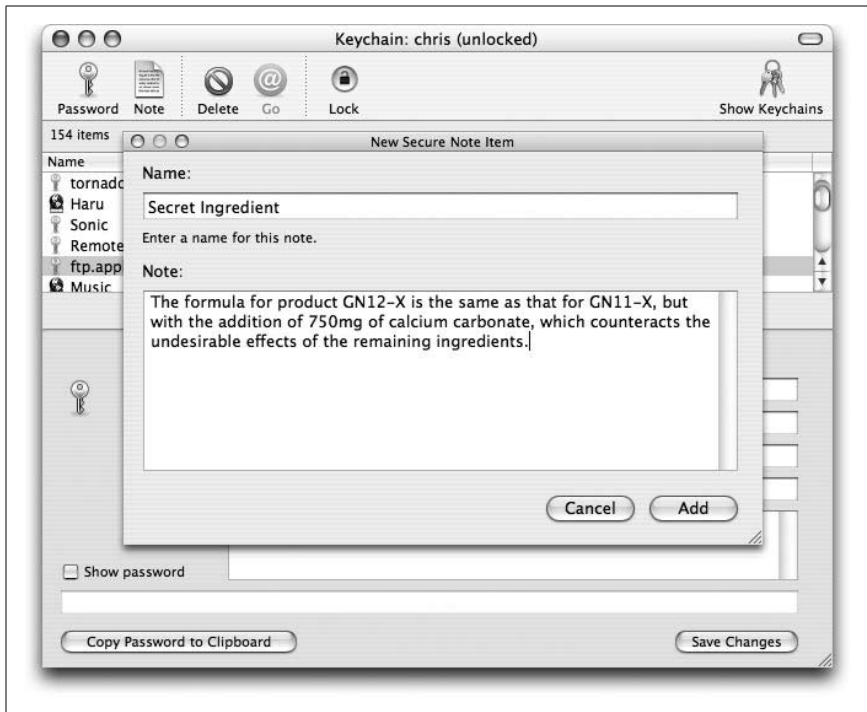


Figure 13-2. Creating a Secure Note with Keychain Access

To access a saved Secure Note, select it from the list of Keychain items, and then from the item's Attributes tab, check the Show Note checkbox. You'll be prompted at least the first time for your keychain password before the text is displayed.

## Password Strength Indicator

The keychain is only as secure as the password you set for it, so receiving feedback when choosing a password can help you optimize security greatly. To view this feedback, choose to change your Keychain password from the Edit menu. Click the Info button (the one with the small "i") at the bottom left of the Change

Keychain Password window, and the Password Assistant window will appear, as shown in Figure 13-3.

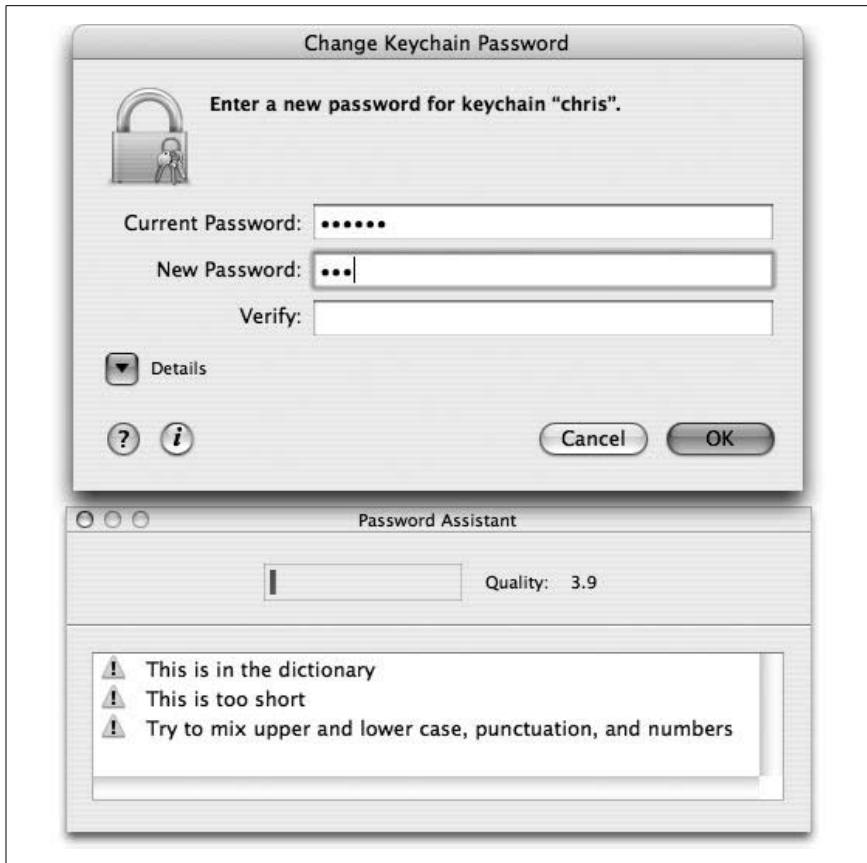


Figure 13-3. Checking password security with the Password Strength Indicator

The Password Assistant's Password Strength Indicator judges your password by several criteria, including length, character variety, and whether it exists in its dictionary (or is close to a word that does), and it alerts you to each issue that applies. A general rating also appears, both as a colored bar gauge running from red to yellow to green (from least to most secure) and as a numerical Quality rating.

## Open Firmware Password

Even though Panther's out-of-the-box security protects it well from network attack and casual entry attempts from the keyboard, there are still ways a determined intruder can access your data as long as the computer is physically accessible. For example, someone can simply attach an external FireWire drive

and, using the Startup Manager by pressing option during startup, select to boot from it.

Likewise, your Mac can be rebooted into target disk mode and get attached to another machine, where it would mount like any other external drive. In both cases, the perpetrator needs only to turn off permissions for the mounted drive (your startup drive) to access all its data. Even easier, your machine can be booted from a Mac OS X installation CD, which allows a user to reset any or all passwords on that machine.

Fortunately, setting an Open Firmware Password can prevent all these scenarios.\* The simplest way to do this is with Apple's Open Firmware Password application (download information is available from <http://docs.info.apple.com/article.html?artnum=120095>). Once a password is set with this utility, shown in Figure 13-4, booting is possible only from the current startup drive unless a password is provided to the Startup Manager. Also, none of the other startup keys will work, including C (to boot from a CD), N (from a NetBoot server), or T (into target disk mode). Setting the password also prevents anyone from booting into single-user or verbose mode, and from resetting the PRAM or Open Firmware.



Figure 13-4. Setting the Open Firmware password

For even greater protection, you can configure Open Firmware to not boot the machine without proper authentication; doing so requires several steps:

\* This isn't supported by all Macintosh models that can run Panther, for example, tray-loading iMacs or Blue & White G3s. See the article at <http://docs.info.apple.com/article.html?artnum=106482> for more information.

1. Boot your Mac into Open Firmware using the Option-⌘-O-F keyboard shortcut during startup. If you've not yet set an Open Firmware password, you can do so at the Open Firmware prompt by typing password and entering a password twice when prompted.
2. Change the value of Open Firmware's *security-mode* variable, which can hold one of three values: none (every machine's default value), command (the value used by the Open Firmware Password application), or full.
3. To prevent booting without a password, set the value to full with this command: `security-mode full`.
4. Enter the command `reset-all`, which restarts the computer.

Subsequent startups, then, will only go as far as the open firmware screen until you first press Enter and then type the password when prompted. At the next prompt, enter the `mac-boot` command, and the Mac will continue its startup normally.

To return the machine to its default boot behavior, set Open Firmware's *security-mode* variable back to none. If you forget the password and are unable to access Open Firmware, your only resort is to reset Open Firmware by changing the amount of installed memory (either add or remove a memory module), and then resetting the PRAM.

## Kerberos and Single Sign-on

Kerberos is a network authentication protocol developed by MIT to allow applications to identify users over open and insecure networks. It's used by governments, large corporations, and higher education. Kerberos is also the native authentication protocol of Active Directory. Since Jaguar, Apple has been moving aggressively to support Kerberos in both Mac OS X Server and Mac OS X, as well as in all the Mac OS X password-using applications, such as Mail, FTP, SSH, and Apple File Sharing. The reason Apple is making this push is to enable single sign-on.

*Single sign-on* means that after a user enters a name and password in the login window, every application on the system that needs to authenticate itself for a network service can do so automatically without requiring the user to enter a different username and password.

For users of Mac OS X, Kerberos is either configured for your network and just works out of the box, or there is a bit of configuration work to be accomplished. If your network falls into the second category, you need to get some information from your system administrator.

## Auto Login

Allowing automatic login at startup is obviously a great security risk, especially if you can't control physical access to the computer. Even a home desktop machine can become portable during a burglary, and allowing auto login makes all your data easily available to the thieves. Because this is Panther's default setting, it's best disabled to ensure even the minimum of protection from unwanted access.

To do so, go to the Security preferences pane, and check the Disable automatic login checkbox.

## Filesystem Security

Even with protections in place preventing unauthorized account access, your Mac is still prone to intrusion as long as there's no filesystem protection in place.

### FileVault

Your entire filesystem can become accessible to anyone able to mount it as an external drive on a second system. This can occur, for example, if your Mac is put into target disk mode and mounted, or more drastically, if your hard drive is removed and placed in another machine. One way to keep at least your home directory safe from intrusion, even in these cases, is to use FileVault, as discussed in Chapter 4.

FileVault also protects your Home directory from intrusion by other users with admin accounts on the same Mac as yours, who could otherwise use *su* or *sudo* to gain access to any file. As long as you're not logged in, your home directory contents stay encrypted and inaccessible to anyone without your account password or the master password. While a FileVault protected account is logged in, however, its home directory resides unencrypted on the drive, subject to access by anyone with an admin account.

Enabling FileVault does incur some risk, however, because the entire Home directory (when not in use) exists as a single encrypted image file on the hard drive. If that single file becomes corrupted, that image and all the files within can be lost. For this reason, you might want to keep a separate account, used for only sensitive work, with FileVault enabled. Doing so results in a smaller image file that's less prone to corruption and more easily backed up.

### Encrypted Images

As an alternative to having FileVault encrypt your entire Home directory, you can instead protect a select group of files by storing them in an encrypted image of your own making. You can do this using either the Disk Utility application or the *hdiutil* command-line utility. Both tools allow you to make sparse image files, which grow as data is added. Normal images, on the other hand, will always use up the amount of space on disk equal to their prespecified capacity.

To create an encrypted disk image, select Images→New→Blank Image from Disk Utility's menus. Name the image file, and specify a save location. Specify in the Size pop-up menu the maximum size to which you would like the image to grow. Select AES-128 from the Encryption pop-up menu and sparse disk image from the Format pop-up, as shown in Figure 13-5. Click OK, and enter a password as prompted. Disk Utility then creates and mounts the image file.

You can create the same image file from the Terminal with the following command:

```
chris$ hdiutil create -type SPARSE -encryption -size 1g -fs HFS+ TopSecret
```

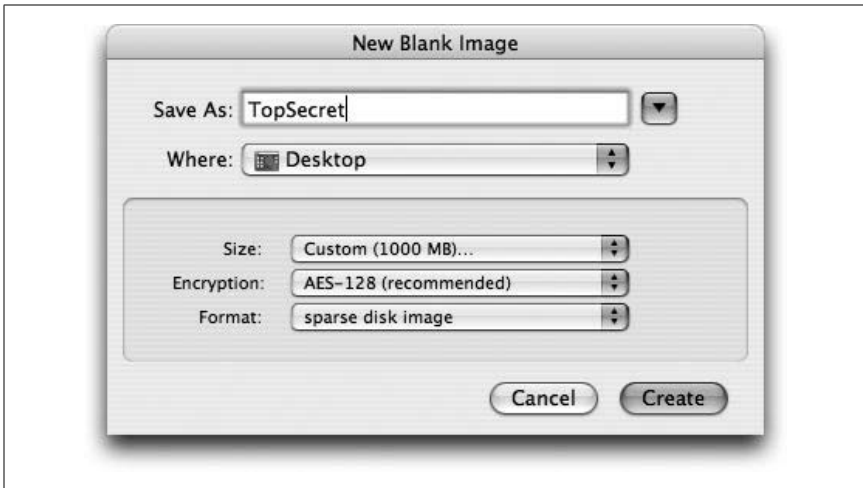


Figure 13-5. Creating an encrypted disk image with Disk Utility

This command creates an encrypted disk image file, named *TopSecret.sparseimage*. Once mounted, the disk image expands to hold up to a gigabyte of data. For more on the *hdiutil* command, see its entry in Chapter 28.

Once you mount an encrypted disk image, you can add data to it like any other volume. When unmounted, however, the disk image stores its data in an encrypted form, accessible only if you can give the appropriate password.

## Secure Deletions

Whether you use the Finder's Trash or the *rm* command to delete a file, the only data that is directly changed on the drive is the entry in the filesystem's directory that points to that file; the file's data still remains on the drive. This means that someone with the right tools can still read bits and pieces of those files, if not resurrect the file in its entirety.

Preventing this exposure, then, means overwriting with other data those drive blocks that hold the residual data, ideally not just once, but several times. Panther provides three ways to do this:

### Secure Empty Trash

Choosing this command from the Finder's application menu ensures that all file data in the Trash is overwritten seven times with a mix of specified and random data. This process is compliant with Department of Defense security specifications.

### *srm*

This Unix utility is the force behind the Finder's Secure Empty Trash feature, which executes *srm* using its *-m* flag. For faster, but less secure deletions, you can run *srm* in the Terminal with its *-s* flag, which overwrites with just one pass. For maximum security, specify neither *-s* nor *-m*, and *srm* will perform

a 35-pass deletion. For a complete description of *srm*'s options, see its entry in Chapter 28.

### *Disk Utility*

To overwrite all blocks on a drive, including all used and available space, use the “8 Way Random Write Format” option when erasing the disk, available by clicking the Options button on Disk Utility's Erase tab. This option is available only for entire disks, not their individual partitions.

## Physical Security

Even with the described security measures in place, they can be of little value if anyone can sit at your unattended Mac and begin working under your logged-in account. Mac OS X includes several features to prevent such unwanted access.

### Log Out on Idle

The Security Preferences pane contains a checkbox that enables automatic logout after a specified period of inactivity, from 5 minutes to 16 hours. The behavior of this logout is identical to that of a manual logout, prompting you to save any unsaved documents (the logout stops if you don't answer the prompt).

### Screen Locking

Also on the Security Preferences pane is a checkbox to enable screen-locking upon wake from sleep or the screensaver. When enabled, this feature presents an authentication dialog box that prevents display of the desktop until you supply the username and password of any admin user. The dialog box also contains a Switch User button that, when clicked, presents the Login window, allowing other users to log in without disturbing the locked-out account.