OS X 10.6 SNOW LEOPARD: KEYCHAIN ACCESS

MANAGING & UNDERSTANDING KEYCHAIN

MANAGING KEYCHAINS

Mac OS X features a sophisticated system that automatically protects all your authentication assets in encrypted keychain files. Much like service workers might keep a keychain of all the keys needed during their workday, the Mac will keep all your resource passwords, certificates, keys, website forms, and even secure notes in a single secure location.

Every time you allow the Mac to remember a password or any other potentially sensitive item, it will save it to a keychain file. Only your account password remains separate from all the other items saved to your keychains.

Because so many important items end up in keychain files, the keychain files themselves are encrypted with a very strong algorithm: They are impenetrable unless you know the keychain's password. In fact, if you forget a keychain's password, its contents are lost forever. Not even the software engineers at Apple can help you - the keychain system is that secure. Yet, probably the single best feature of the keychain system is that it's entirely automatic using default settings.

Most users will never know just how secure their saved passwords are because the system is transparent.

Understanding Keychain files

There are keychain files stored throughout the system for different users and resources:

/Users/<username>/Library/Keychain/login.keychain—Every standard or administrative user is created with a single login keychain. As a default, the password for this keychain matches the user's account password, so this keychain is automatically unlocked and available when the user logs in. If the user's account password does not match the keychain's password, it will not automatically unlock during login.

Users can create additional keychains if they wish to segregate their authentication assets. For example, you can keep your default login keychain for trivial items, and then create a more secure keychain that does not automatically unlock for more important items.

/Library/Keychain/FileVaultMaster.keychain—This keychain is encrypted with the FileVault master password.

/Library/Keychain/System.keychain—This keychain maintains authentication assets that are non-user-specific. Examples of items stored here include AirPort wireless network passwords, 802.1X network passwords, and local Kerberos support items. Although all users benefit from this keychain, only administrative users can make changes to it.

/System/Library/Keychains/—You will find several keychain files in this folder that store root certificates used to help identify trusted network services. Once again, all users benefit from these keychains, but only administrative users can make changes to these keychains.

NOTE:
Some websites will remember your password inside a web cookie, so you might not see an entry in a keychain file for every website password you save.

Using Keychain Access

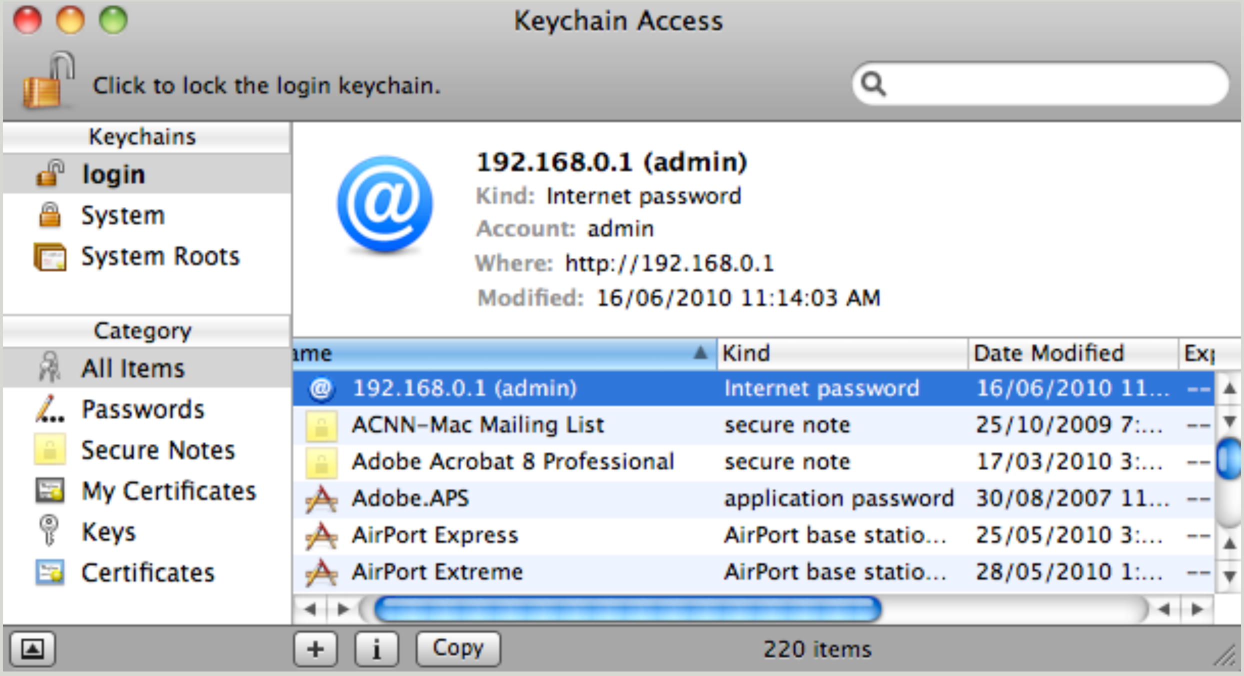
The primary tool you will use to manage keychains is the Keychain Access application found in the /Applications/Utilities folder. With this application you can view and modify any keychain item including saved resource passwords, certificates, keys, website forms, and secure notes. You can also create and delete keychain files, change keychain settings and passwords, and repair corrupted keychains.

Manage Items in a Keychain

To manage keychain items, including saved passwords:

1. As any user, open /Applications/Utilities/Keychain Access.

The default selection will show the contents of the user's login keychain, but you could select another keychain from the list to view its items.



Keychain Access

Click to lock the login keychain.

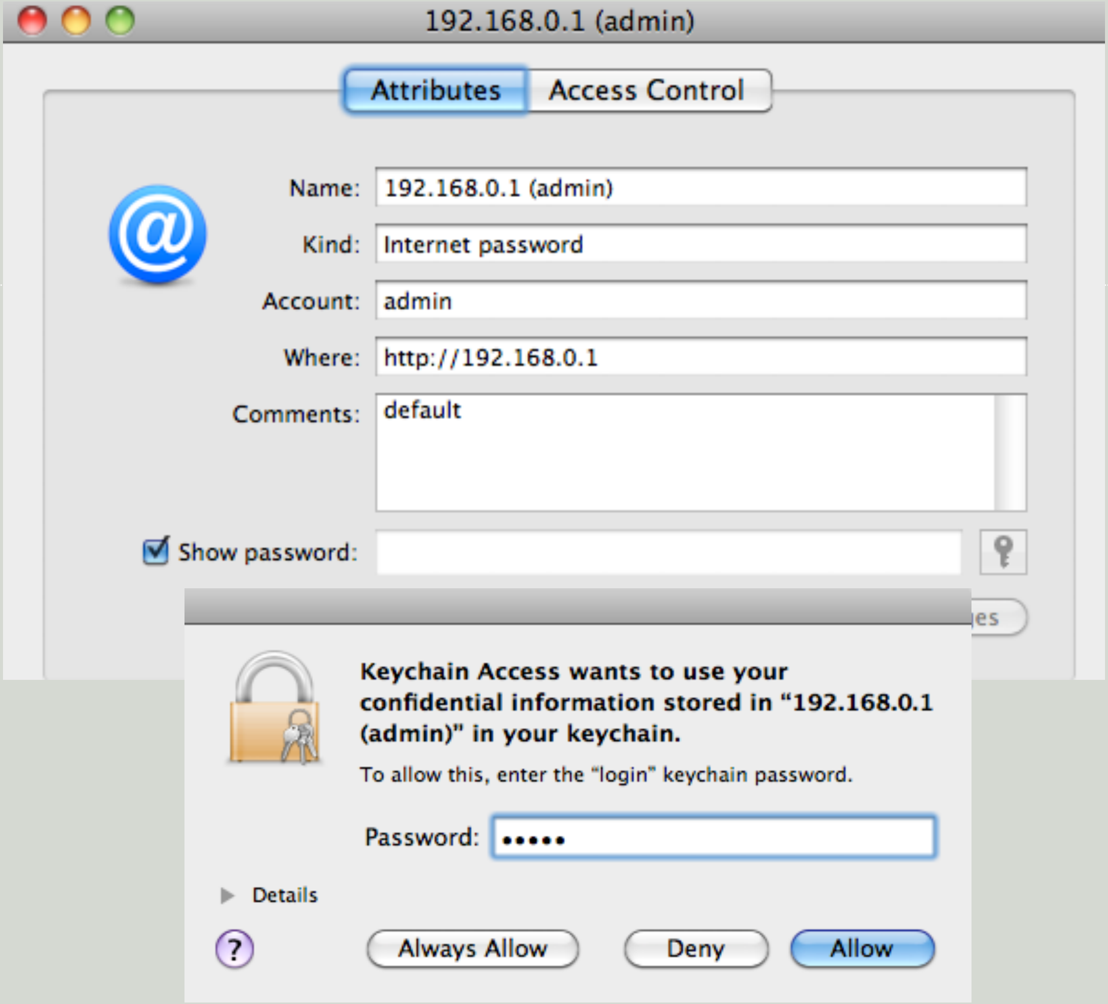
192.168.0.1 (admin)
Kind: Internet password
Account: admin
Where: http://192.168.0.1
Modified: 16/06/2010 11:14:03 AM

ame	Kind	Date Modified	Ex
192.168.0.1 (admin)	Internet password	16/06/2010 11...	--
ACNN-Mac Mailing List	secure note	25/10/2009 7:...	--
Adobe Acrobat 8 Professional	secure note	17/03/2010 3:...	--
Adobe.APS	application password	30/08/2007 11...	--
AirPort Express	AirPort base statio...	25/05/2010 3:...	--
AirPort Extreme	AirPort base statio...	28/05/2010 1:...	--

220 items

2.Double-click a keychain item to view its attributes.

3. If the item is a password, you can reveal the saved password by selecting the “Show password” checkbox.



192.168.0.1 (admin)

Name: 192.168.0.1 (admin)
Kind: Internet password
Account: admin
Where: http://192.168.0.1
Comments: default

☑ Show password:

Keychain Access wants to use your confidential information stored in “192.168.0.1 (admin)” in your keychain.

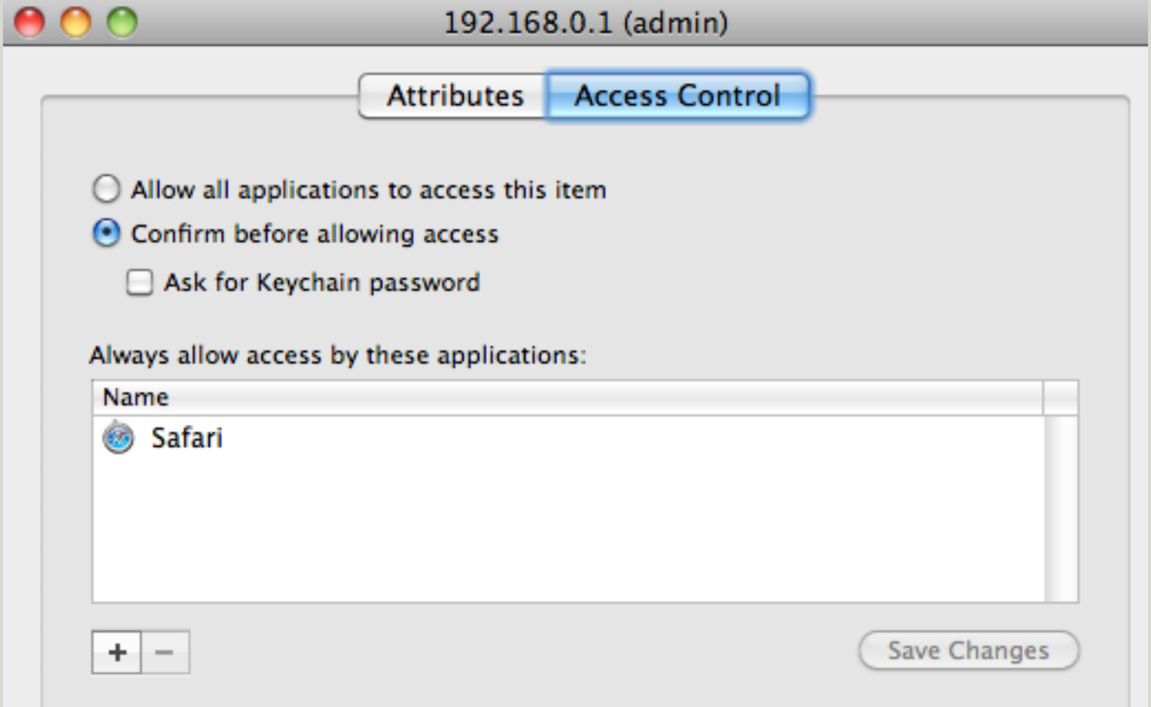
To allow this, enter the “login” keychain password.

Password: •••••

4.When prompted, enter the keychain password once more, and then click the Allow button to reveal the saved password. It is not advisable to click the **Always Allow button**.

Once you have authenticated, you can change any attribute in the keychain item dialog.

5 When you have finished making changes, click the Save Changes button.
6 Finally, you can also click the Access Control tab in the keychain item's attributes dialog to adjust application access for the selected item.


192.168.0.1 (admin)

○ Allow all applications to access this item
● Confirm before allowing access
□ Ask for Keychain password

Always allow access by these applications:

Name
Safari

TIP: To easily search through all the keychain items, use the Categories views to the left or the Spotlight search in the top-right corner of the toolbar.

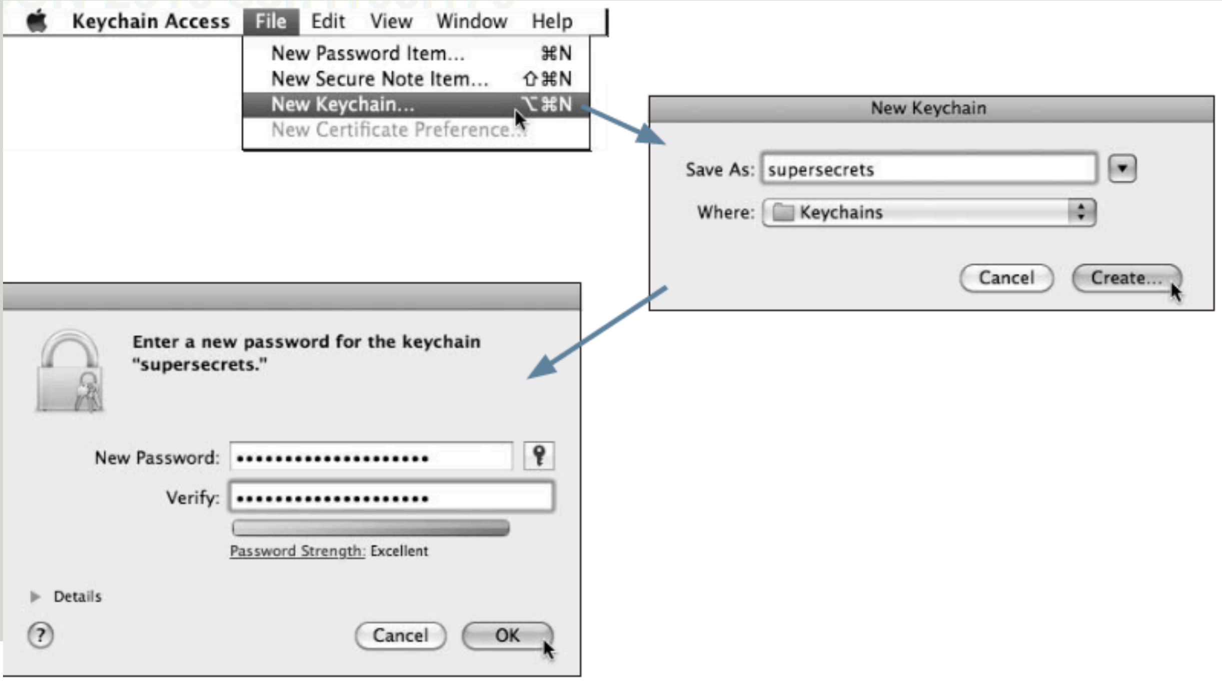
TIP: The safest place to store secure text on your Mac is in keychains. In Keychain Access, you can create a new secure note by choosing File > New Secure Note Item from the menu bar.

Manage Keychain Files

To manage keychain files, including resetting a keychain's password:

1 As any user, open /Applications/Utilities/Keychain Access.

2 To create a new keychain, choose File > New Keychain from the menu bar. Next, enter a name and location for the new keychain. The default location is the Keychains folder inside your home folder. Finish by entering a nontrivial password that is six characters or longer for the new keychain and click the OK button.



New Keychain

Save As: supersecrets

Where: Keychains

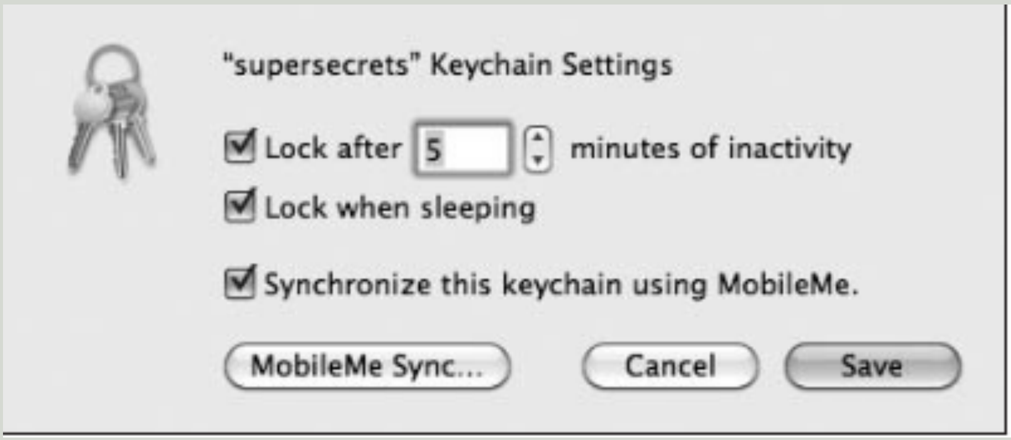
Enter a new password for the keychain "supersecrets."

New Password: ••••••••••••••••••••

Verify: ••••••••••••••••••••

Password Strength: Excellent

3 To change a keychain’s settings, first select it from the list, and then choose Edit > Change Settings for Keychain from the menu bar. You will be able to change automatic keychain locking settings and enable .Mac synchronization. Finish by clicking the Save button.



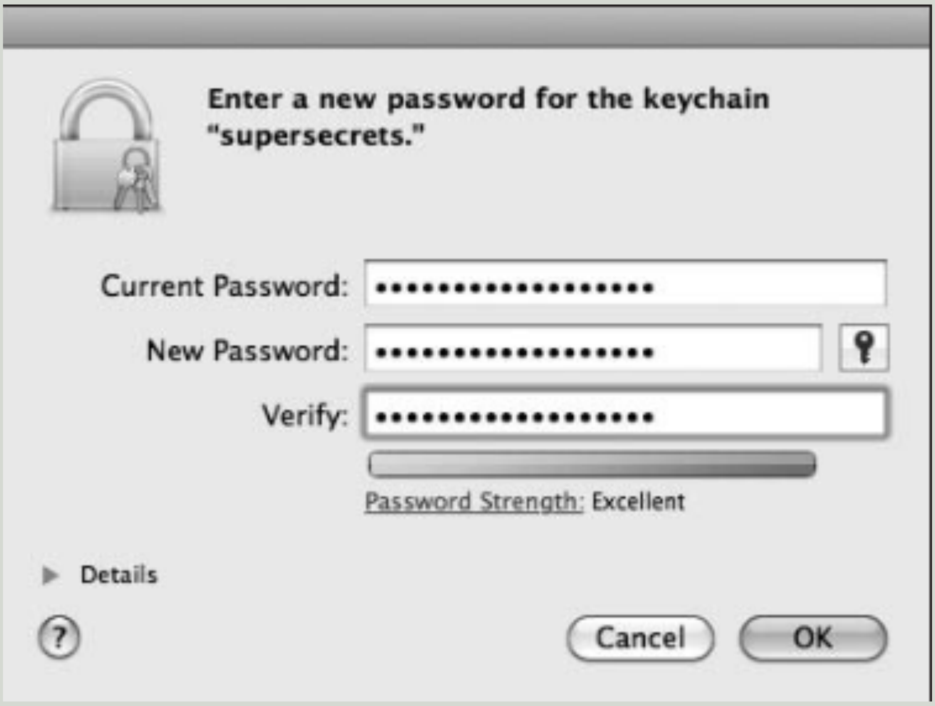
"supersecrets" Keychain Settings

☑ Lock after 5 minutes of inactivity

☑ Lock when sleeping

☑ Synchronize this keychain using MobileMe.

4 To change a keychain’s password, first select it from the list, and then choose Edit > Change Password for Keychain from the menu bar. You will have to enter the keychain’s current password first. Finish by entering a nontrivial password that is six characters or longer and click the OK button.



Enter a new password for the keychain "supersecrets."

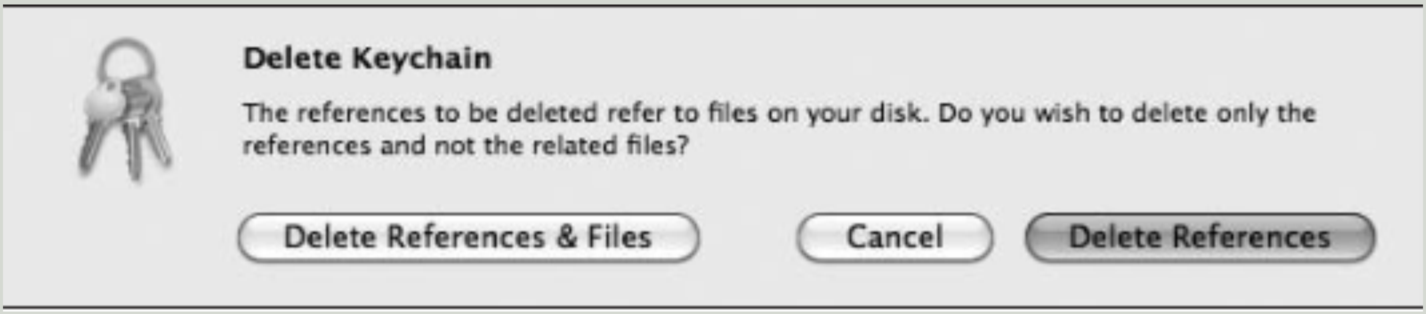
Current Password: ••••••••••••••••••

New Password: ••••••••••••••••••

Verify: ••••••••••••••••••

Password Strength: Excellent

5 To delete a keychain, select it from the list and choose File > Delete Keychain from the menu bar. When the Delete Keychain dialog appears, click the Delete References button to simply ignore the keychain or click the Delete References & Files button to completely erase the keychain file.



Delete Keychain

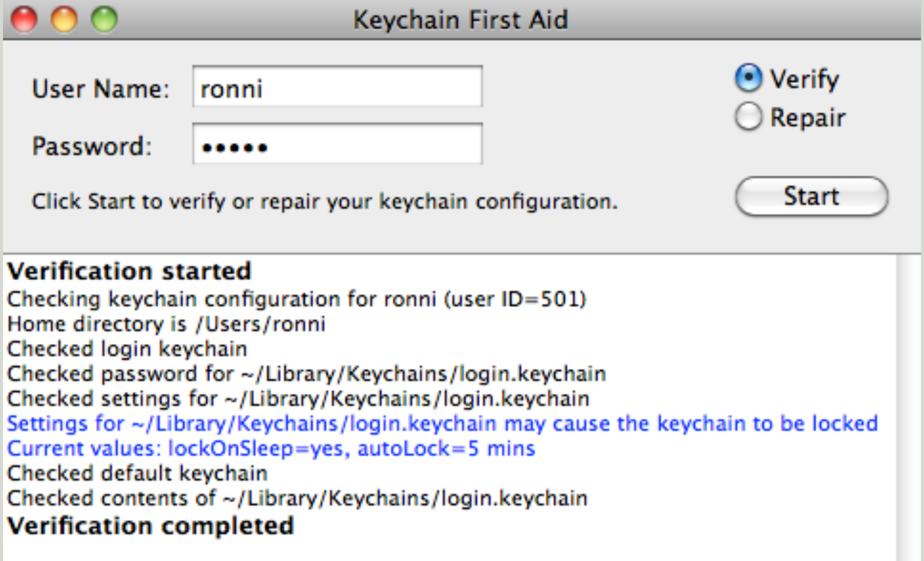
The references to be deleted refer to files on your disk. Do you wish to delete only the references and not the related files?

TIP: You can move keychain items between keychains by dragging and dropping an item from one keychain to another.

TIP: For quick access to your keychains and other security features, you can enable the security menu item by choosing Keychain Access > Preferences from the menu bar. Then select the Show Status in Menu Bar checkbox to reveal the security menu item, as indicated by a small key icon on the right side of the menu bar.

Repair Keychain Files

To verify or repair a keychain file:
1 As any user, open /Applications/Utilities/Keychain Access.
2 If the troublesome keychain is not already in your keychain list, choose File > Add Keychain from the menu bar and you will be able to browse for it.
3 You need to unlock all the keychains you wish to check. Simply select the keychain from the list, then choose File > Unlock Keychain from the menu bar and enter the keychain's password.
4 Choose Keychain Access > Keychain First Aid from the menu bar.
5 You will have to enter your password once more, and then choose the Verify or Repair radio button and finally click the Start button.
A log will show the keychain verification or repair process.



User Name: ronni

Password: •••••

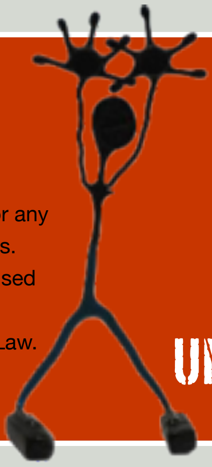
● Verify
○ Repair

Click Start to verify or repair your keychain configuration.

```
Verification started
Checking keychain configuration for ronni (user ID=501)
Home directory is /Users/ronni
Checked login keychain
Checked password for ~/Library/Keychains/login.keychain
Checked settings for ~/Library/Keychains/login.keychain
Settings for ~/Library/Keychains/login.keychain may cause the keychain to be locked
Current values: lockOnSleep=yes, autoLock=5 mins
Checked default keychain
Checked contents of ~/Library/Keychains/login.keychain
Verification completed
```

TIP: Additional Keychain First Aid preferences can be found by selecting Keychain Access > Preferences from the menu bar.

RONNI
JULY 2010



OSX 10.6 SNOW LEOPARD

KEYCHAIN ACCESS

MANAGING &

UNDERSTANDING KEYCHAIN