

# Managing Public Area Macs (OS X)

James Partridge (OUCS)

24 June 2004



# What will this talk cover?

---

- ❑ Overview of integrating OS X into Directory Services
- ❑ Client Management
- ❑ Application Management
- ❑ Essential Tools
- ❑ Security



# Why talk at all?

---

- ❑ Still many preconceptions about MacOS X dating from OS 9 days
- ❑ Macs are very well suited to Help Centres
- ❑ More detailed courses (esp. on Directory Service integration) will be offered



# Directory Service Integration

- ❑ AD
- ❑ eDir
- ❑ Should I use an OS X Server?



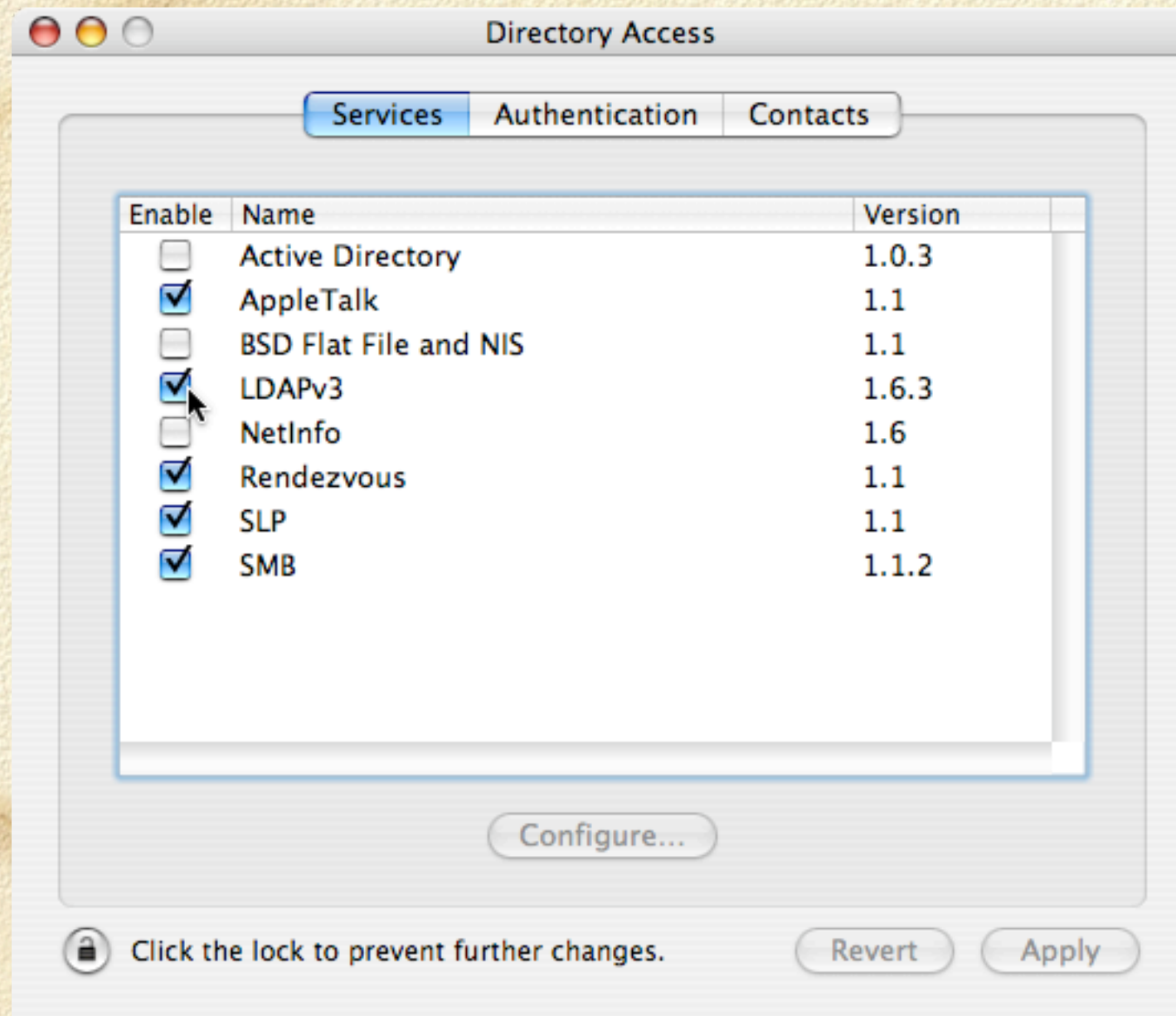
# Active Directory

---

- ❑ We aren't even at the testing stage yet
- ❑ 10.3 native authentication uses the AD plug-in in Directory Access.app
- ❑ ADmitMac (Thursby) is popular. Thursby's comparison of ADmitMac and the native 10.3 AD method is available at: <http://www.thursby.com/products/admitmac-vs-panther.html>
- ❑ 10.3 native plug-in good for smaller environments; ADmitMac better for larger ones
- ❑ Useful scripts at <http://shukwit.com/> and other documentation on Macosxlab's site



# eDirectory



- ❑ No native eDir plug-in (yet!!)
- ❑ Must extend eDir schema to accommodate Macs
- ❑ Use LDAPv3 and custom mappings on the client



| Netware 5.1                               | Netware 6                           | Netware 6.5                                   |
|---|-------------------------------------|---|
| Native File Access pack must be installed | Native NFAP or can be added         | Native NFAP or can be added                   |
| AFP 2.2                                   | AFP 2.2                             | AFP 3.1                                       |
| NDS RSA + Simple password                 | NDS RSA + Simple password           | Universal password                            |
| $\leq 8$ character passwords on Mac       | $\leq 8$ character passwords on Mac | $\geq 8$ character passwords on Mac (in SP2?) |



# eDir Authentication Summary

---

- ❑ Extend schema (LDIF files are available for NW6 and NW6.5)
- ❑ Set user attributes
- ❑ Create mounts object
- ❑ Import server public certificate (for SSL connections) onto client Mac (convert from .der to .pem format)
- ❑ Directory Access for LDAP mappings
- ❑ Diagnose problems



# Server Public Certificate

---

- ❑ Copy RootCert.der file from SYS:PUBLIC directory on NW server into folder on client Mac
- ❑ Open Terminal.app, navigate to folder and type: `openssl x509 -inform DER -outform PEM -in RootCert.der -out RootCert.pem`
- ❑ Create directory 'certs' in /Library, then `sudo cp [path]/RootCert.pem /Library/certs`
- ❑ `cd /Library/certs`, then: `sudo chown root:wheel RootCert.pem` and `sudo chmod 400 RootCert.pem`
- ❑ Add the following line to /etc/openldap/ldap.conf: `TLS_CACERT /Library/certs/RootCert.pem`



# Netware Troubleshooting

---

- ❑ SDIDIAG to check only one SDI key for Tree
- ❑ Monitor LDAP activity with DSTRACE:
  - ❑ DSTRACE SCREEN ON
  - ❑ DSTRACE -ALL
  - ❑ DSTRACE +LDAP
- ❑ Pipe DSTRACE activity into a file with DSTRACE FILE ON (defaults to SYS:\System)



# Netware Troubleshooting

---

- ❑ Monitor NMAS activity with NMAEMON:
  - ❑ NMAEMON \* sys:\public\mmaslog.txt
  - ❑ Turn it off with UNLOAD NMAEMON
- ❑ AFP activity: AFPPLOG ON / AFPPLOG OFF
  - ❑ Creates log file afptcp.log in SYS:\ETC



# Should I use OS X Server?

---

- ❑ 10 or unlimited client versions are available
- ❑ Doesn't require an Xserve to run - any reasonable Mac will do
- ❑ LDAP integration into existing Directory Services
- ❑ Excellent client management (OS X & OS 9)
- ❑ Many other uses



# OS X Client Management

- ❑ ARD
- ❑ Radmin
- ❑ Casper
- ❑ OS X Server



# Apple Remote Desktop 1.2

---

- ❑ Current version
  - ❑ Good for monitoring and troubleshooting
  - ❑ Quite secure: AES-128 bit encryption; uses UDP 3283
  - ❑ Uses Apple's own ARD protocol
  - ❑ Can be started remotely with the 'kickstart' utility: `sudo '/System/Library/CoreServices/ARD Agent.app/Contents/Resources/kickstart' -restart -agent`
- ❑ See <http://www.apple.com/support/remotedesktop> for more details



# Apple Remote Desktop 2

---

- ❑ New version ARD 2 (available in July)
  - ❑ Greatly enhanced management capabilities
  - ❑ Single and multiple software installs (can be scheduled)
  - ❑ Greatly enhanced inventory db (PostgreSQL) & reporting
  - ❑ Uses VNC (so can view Linux and Windows too); Java viewer also built in
  - ❑ Execute Unix shell scripts or commands on 1 or more Macs
  - ❑ ...and many more! (comparison chart at <http://www.apple.com/uk/remotedesktop/upgrade.html>)



# Radmind

---



- ❑ Powerful CLI Unix tools (a Tripwire system, in effect)
- ❑ Open Source
- ❑ `http://rsug.itd.umich.edu/software/radmind/`
- ❑ Several webcasts on the Macosxlabs site: `http://www.macosxlabs.org/webcasts/index.html`
- ❑ Widely used in academic institutions, but has a relatively steep learning curve



# Casper 2

---

- Several Parts:

- Casper Admin



- Casper



- Composer



- Recon



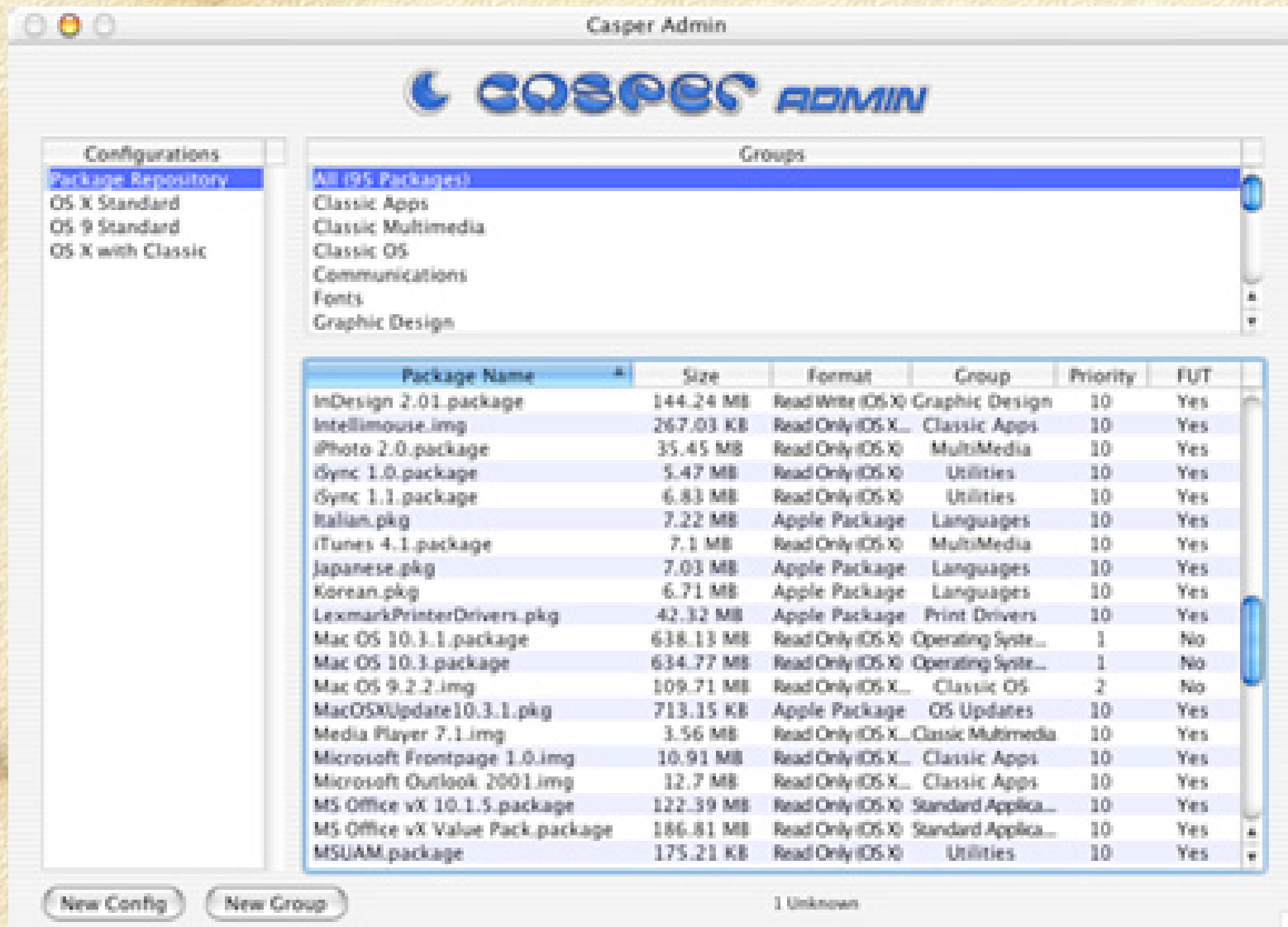
<http://www.jamfsoftware.com/index.html>



# Casper Admin

Application packages can be bundled together into groups (e.g., Web browsers).

Packages and Groups can be bundled together to make Configurations (e.g., for specific Colleges or Departments)





# Casper

---

Client-side application for deploying packages to client machines

Can be run from local FireWire drive or from an OS X server hosting NetBoot images

Can push packages to remote machines (over SSL)

Can be used for deploying a standard OS X image





# Recon

Recon for JAMF Demo

Please fill out the information about your computer below

|                    |  |                   |   |
|--------------------|--|-------------------|---|
| User's Name:       | <input type="text" value="Benny"/>           | Computer Name:    | <input type="text" value="Benny's Computer"/>   |
| Phone Number:      | <input type="text"/>                         | Asset Tag:        | <input type="text" value="387624"/>   |
| Email Address:     | <input type="text" value="benny@email.com"/> | Position:         | <input type="text" value="Assistant"/>  |
| Department:        | <input type="text" value="Development"/>     | Room:             | <input type="text" value="100a"/>   |
| Building:          | <input type="text" value="Fleming Hall"/>    |                   |   |
| Monitor Make:      | <input type="text" value="Apple"/>           | Monitor Model:    | <input type="text"/>  |
| Monitor Size:      | <input type="text" value="21"/>              |                   |   |
| Monitor Asset Tag: | <input type="text" value="387625"/>          | Monitor Serial #: | <input type="text"/>  |
| PO Number:         | <input type="text" value="100345"/>          | PO Date:          | <input type="text" value="02"/> / <input type="text" value="22"/> / <input type="text" value="2003"/> |
| Vendor:            | <input type="text" value="Apple"/>           | Warranty Expires: | <input type="text" value="02"/> / <input type="text" value="22"/> / <input type="text" value="2006"/> |

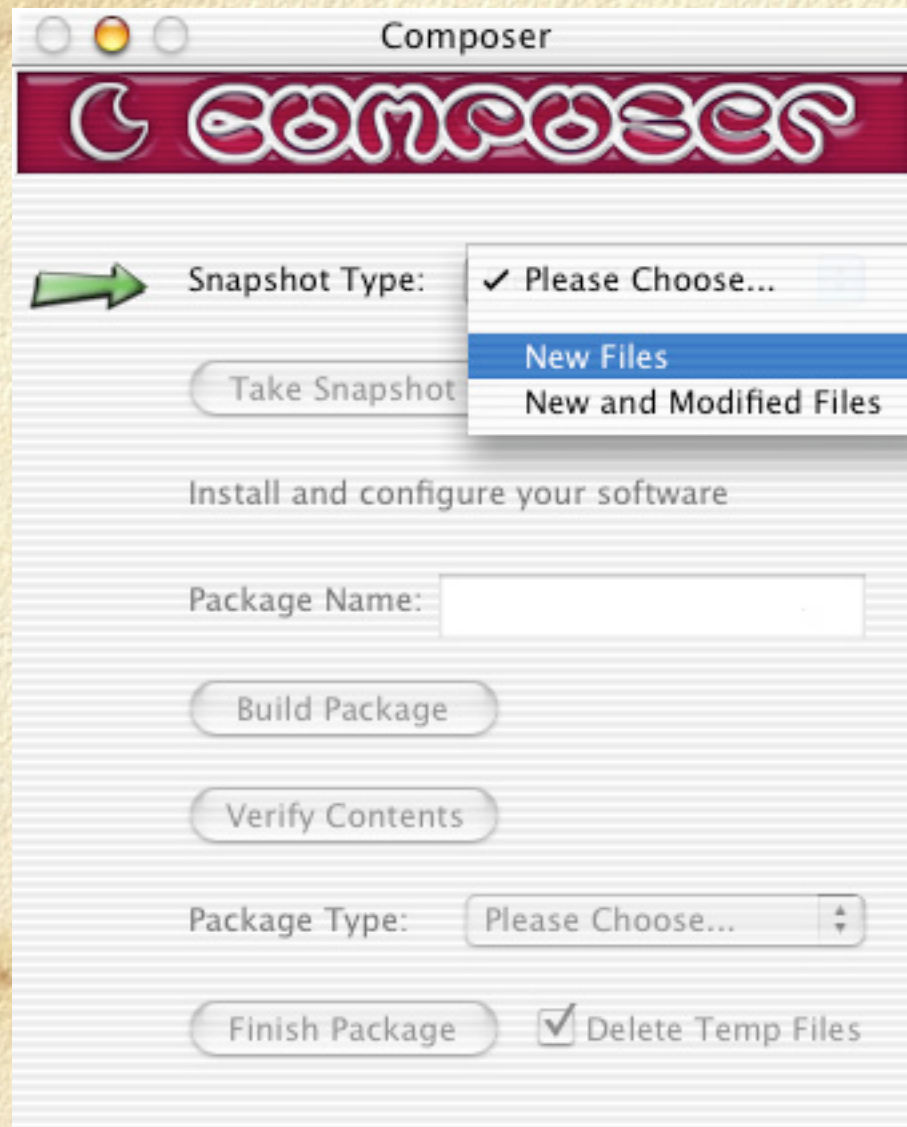
Communicates  
with Jamf Software  
Server to upload  
hardware &  
software inventory





# Composer

---



Builds packages for  
deployment by Casper

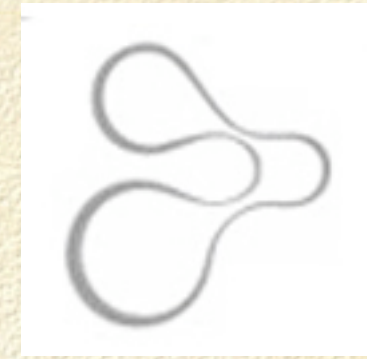
Takes before and after  
snapshots of an install





# Jamf Software Server

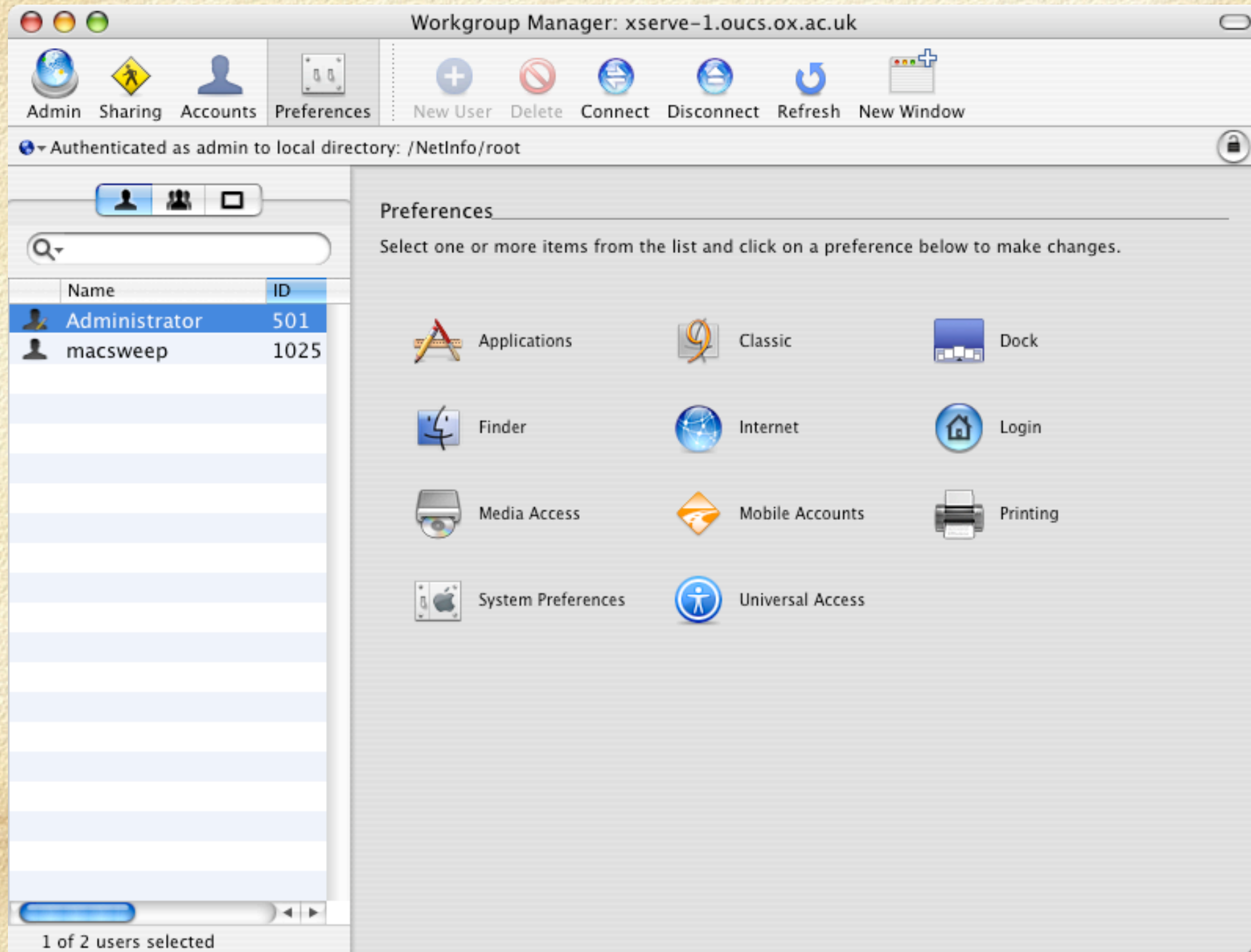
---



- ❑ Web interface to Casper
- ❑ Apache Tomcat / MySQL backend
- ❑ Can be installed and configured in a few minutes
- ❑ Combines Casper, Casper Admin, Recon and Composer



# OS X Server





# Application Management

- ❑ Installers
- ❑ CLI
- ❑ Licensing



# Application Installers

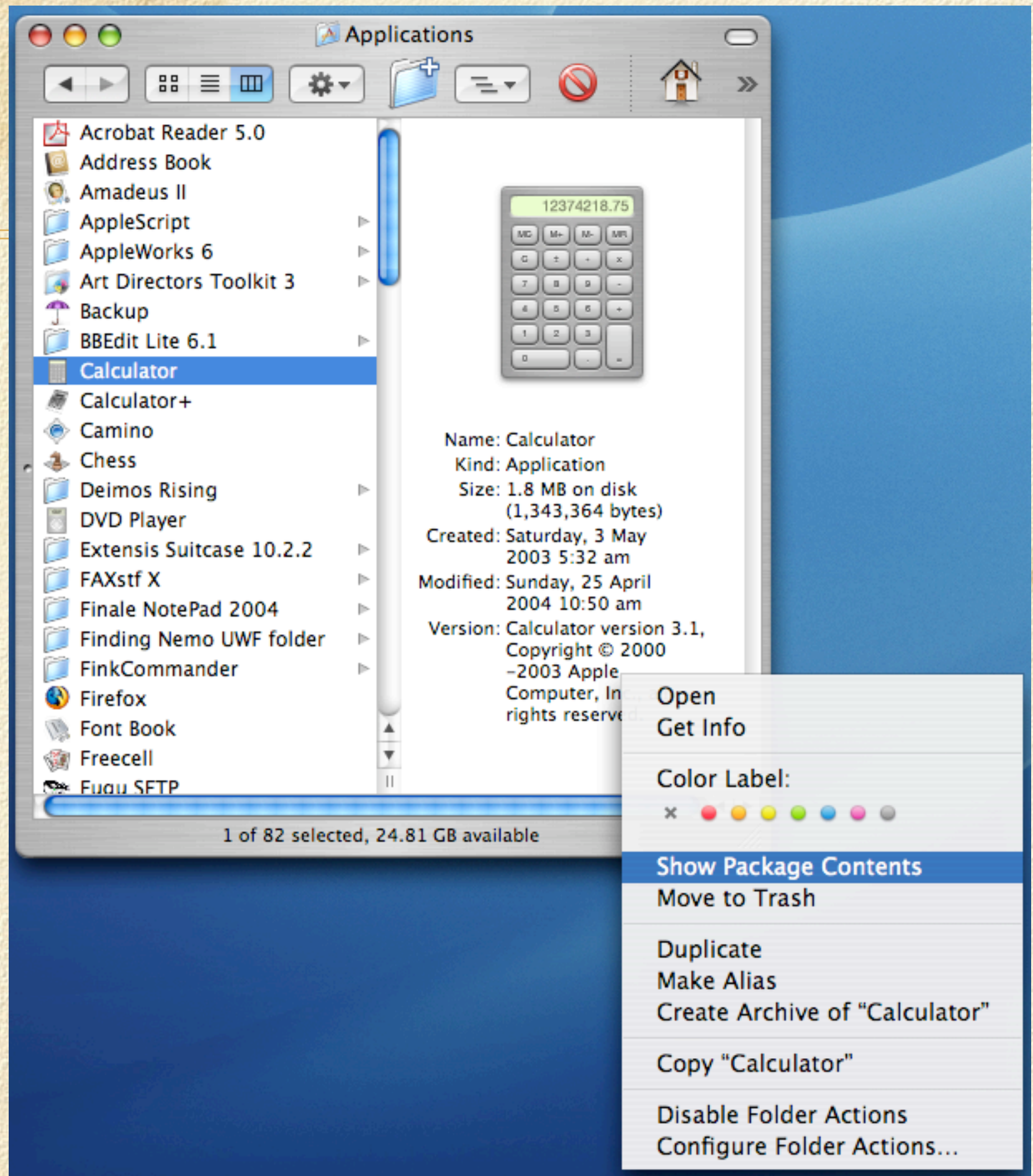
---

- Read the new white paper on the Macosxlabs site: “Mac OS X Enterprise Application Management: Best Practices”
- Utah University have a very helpful site: <http://www.macos.utah.edu/crappyApps.html>
- Understand different types of Application install in OS X



# Application Bundles

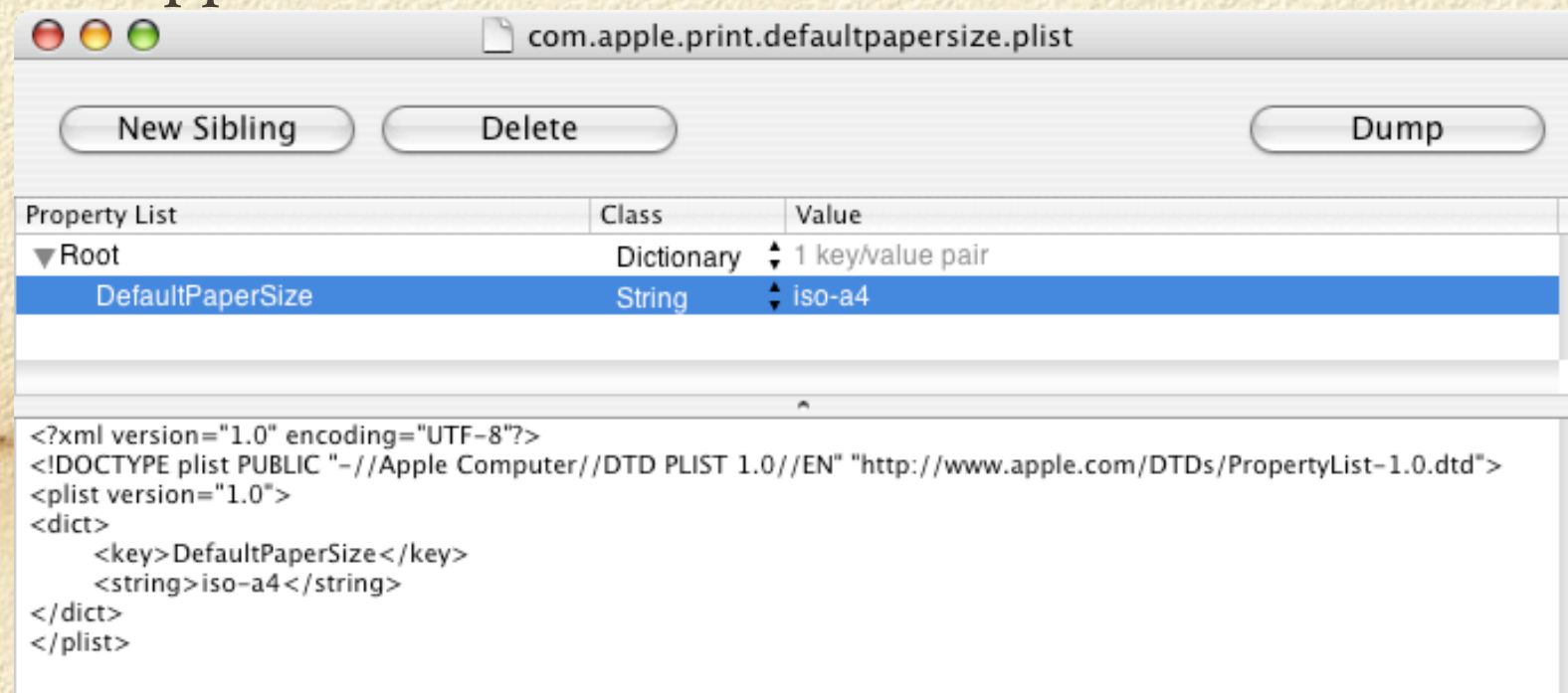
- Many OS X apps are, more correctly, application *bundles* or *packages*. Actually, they're folders.
- Bundle contents can be seen by **control-click** on app name, then selecting 'Show Package Contents'





# .plist files (~/.Library/Preferences)

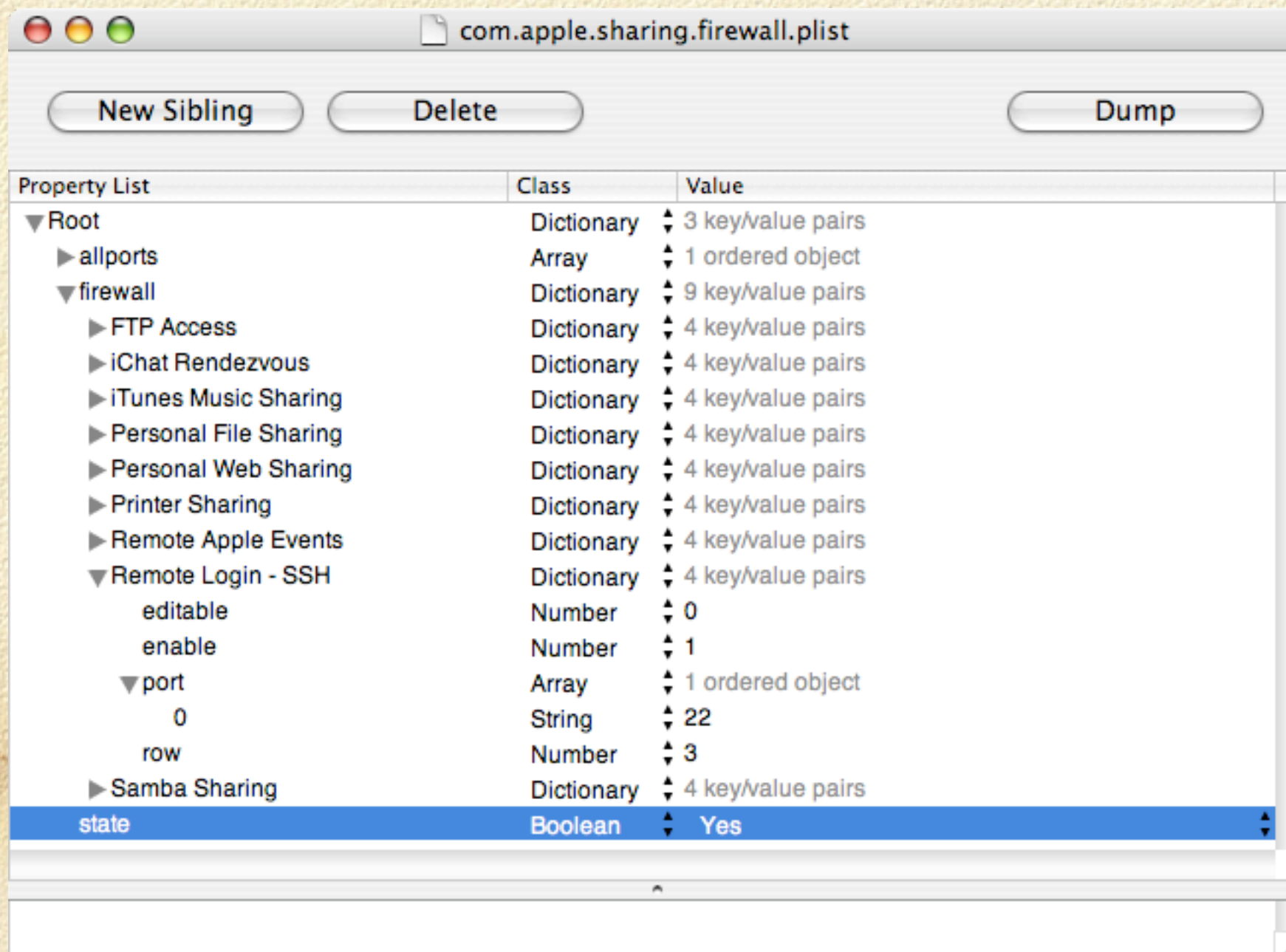
- ❑ .plist files are XML files containing all User or Application preferences. Think of them as configuration files
- ❑ User-defined .plist files in ~/.Library/Preferences can be deleted or edited fairly safely. Check for syntax errors with `sudo plutil -s ~/.Library/Preferences/*.plist`
- ❑ can be read (e.g., `defaults read -app Safari`) or edited (e.g., `defaults write com.apple.Safari IncludeDebugMenu 1`) in terminal.app. See `man defaults` for more info.





# .plist files (/Library/Preferences)

- These will override preference files in ~/Library/Preferences if the same





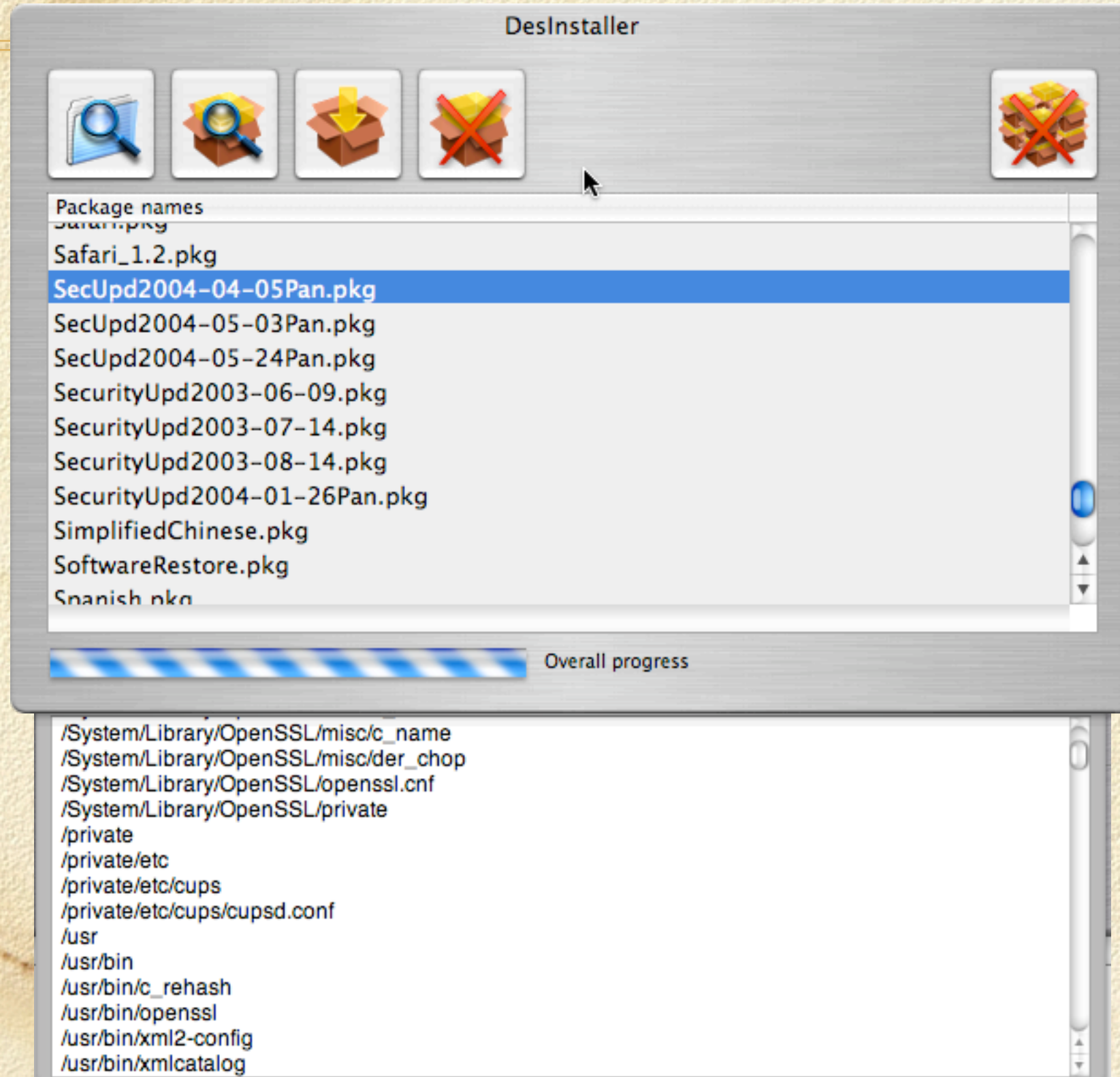
# Uninstalling

---

- ❑ In most cases, simply drag app to Trash
- ❑ .plist files may be left in `~/Library/Preferences` but these are tiny and harmless and can be deleted or left
- ❑ Some apps are messier. **DesInstaller** is a big help (but use with caution). Download it from <http://krugazor.free.fr/software/desinstaller/DesInstaller.php> (free)
  - ❑ DesInstaller reads the Package Receipts in `/Library/Receipts`
  - ❑ The `lsbom` tool shows the same info (**man lsbom**)
- ❑ Management apps such as Radmind can do this too



# DesInstaller





# Tools

---

- ❑ Carbon Copy Cloner
- ❑ FW Drive



# Carbon Copy Cloner

---

- ❑ Mike Bombich is highly respected in the Mac community
- ❑ Fantastic tool: use for backup and restore of clean installs
- ❑ Use for cloning and distributing known systems
- ❑ Clone volume before repartitioning drive
- ❑ Free for Education (otherwise donation ware)

<http://www.bombich.com/software/ccc.html>



# FireWire

---



- Two speeds: 400 and 800 Mbps
  - New drives have both + USB2
- Cheap cables are frequent cause of problems - buy good ones
- **Always** dismount drives cleanly before unplugging (⌘e)
- Check devices in System Profiler
- Blue & White G3 Macs *cannot* boot from FireWire drives, most others can



# Essential Software

---

- ❑ Install CDs
- ❑ Alsoft Disk Warrior
- ❑ CCC (Carbon Copy Cloner)
- ❑ TechTool Pro
- ❑ Norton Utilities





# Major OS X Disk Utilities

---



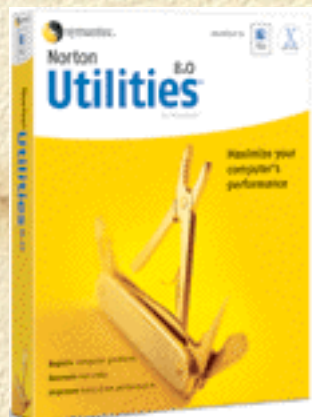
- DiskWarrior 3.0 (with CD updater)

• <http://www.alfsoft.com/DiskWarrior/index.html>



- TechTool Pro v.4

• <http://www.micromat.com/>



- Norton Utilities 8.0

• [http://www.symantec.com/nu/nu\\_mac/index.html](http://www.symantec.com/nu/nu_mac/index.html)



# Maintenance tools:

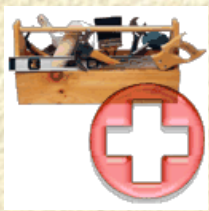
---



**Onyx:** <http://www.titanium.free.fr/english/onyx/index.html>



**Xupport:** <http://www.computer-support.ch/Xupport/index.html>



**TinkerTool / TinkerTool Pro:**  
<http://www.bresink.com/osx/index.html>



**Cronnix:** <http://www.koch-schmidt.de/cronnix/>

Also Rans:

**Panther Cache Cleaner** (<http://www.northernsoftworks.com/panthercachecleaner.html>)

**MacJanitor** ([http://personalpages.tds.net/~brian\\_hill/macjanitor.html](http://personalpages.tds.net/~brian_hill/macjanitor.html))



# Security

---



# Open Firmware



For Macs in a public area it's a good idea to password protect the Open Firmware. This prevents:

- ☐ Startup from CD (c)
- ☐ Startup from Network (n)
- ☐ Startup in Target Disk Mode (t)
- ☐ Startup in Single User ( $\text{⌘s}$ ) or Verbose ( $\text{⌘v}$ ) Mode
- ☐ Blocks a PRAM reset ( $\text{⌘}\text{⌘pr}$ )
- ☐ Access to Open Firmware ( $\text{⌘}\text{⌘of}$ ) blocked without password
- ☐ Password required for Startup Manager ( $\text{⌘}$ )



# Anti-Virus Software

---

- ❑ You need it, even though there are still **NO** OS X viruses or worms (proof-of-concepts aside)
- ❑ Sophos client [update - July 2004]
  - ❑ New 10.2+ client no longer requires mounted volume on desktop
  - ❑ New 10.2+ client updates automatically from CID
  - ❑ Can't be managed by Savadmin
  - ❑ AFP-enabled sharepoint on Windows server necessary for EM Library