



# Managing Tigers

John DeTroye  
Sr. Consulting Engineer  
Apple Education  
johnd@apple.com

<https://developer.apple.com/wwdcsecure/>

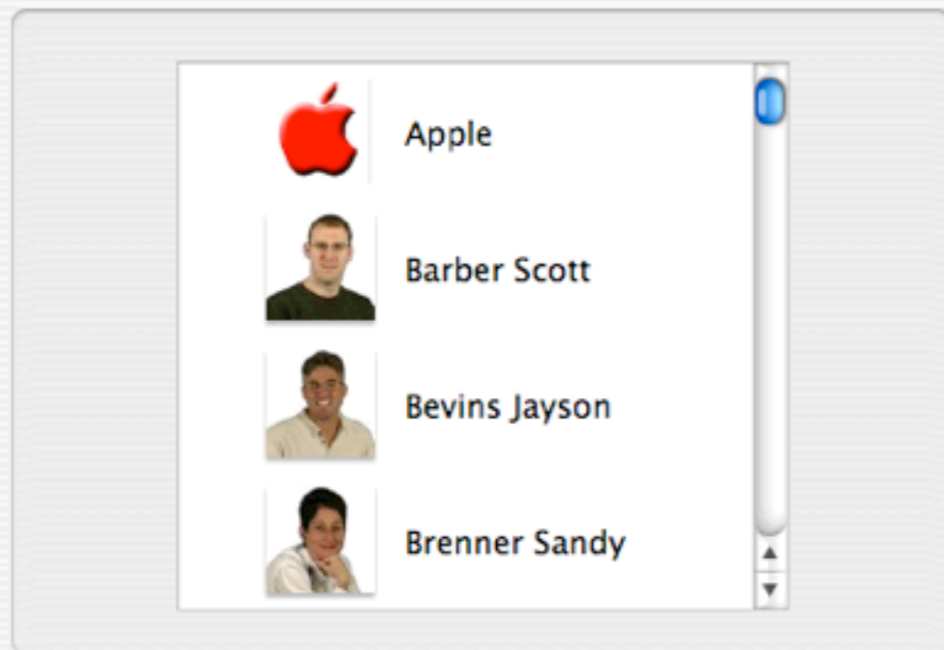




## Mac OS X

● Network Accounts Available

Managed Lab Client  
Play nice and be good to Tenshi  
(That means give her treats...)



Sleep



Restart



Shut Down

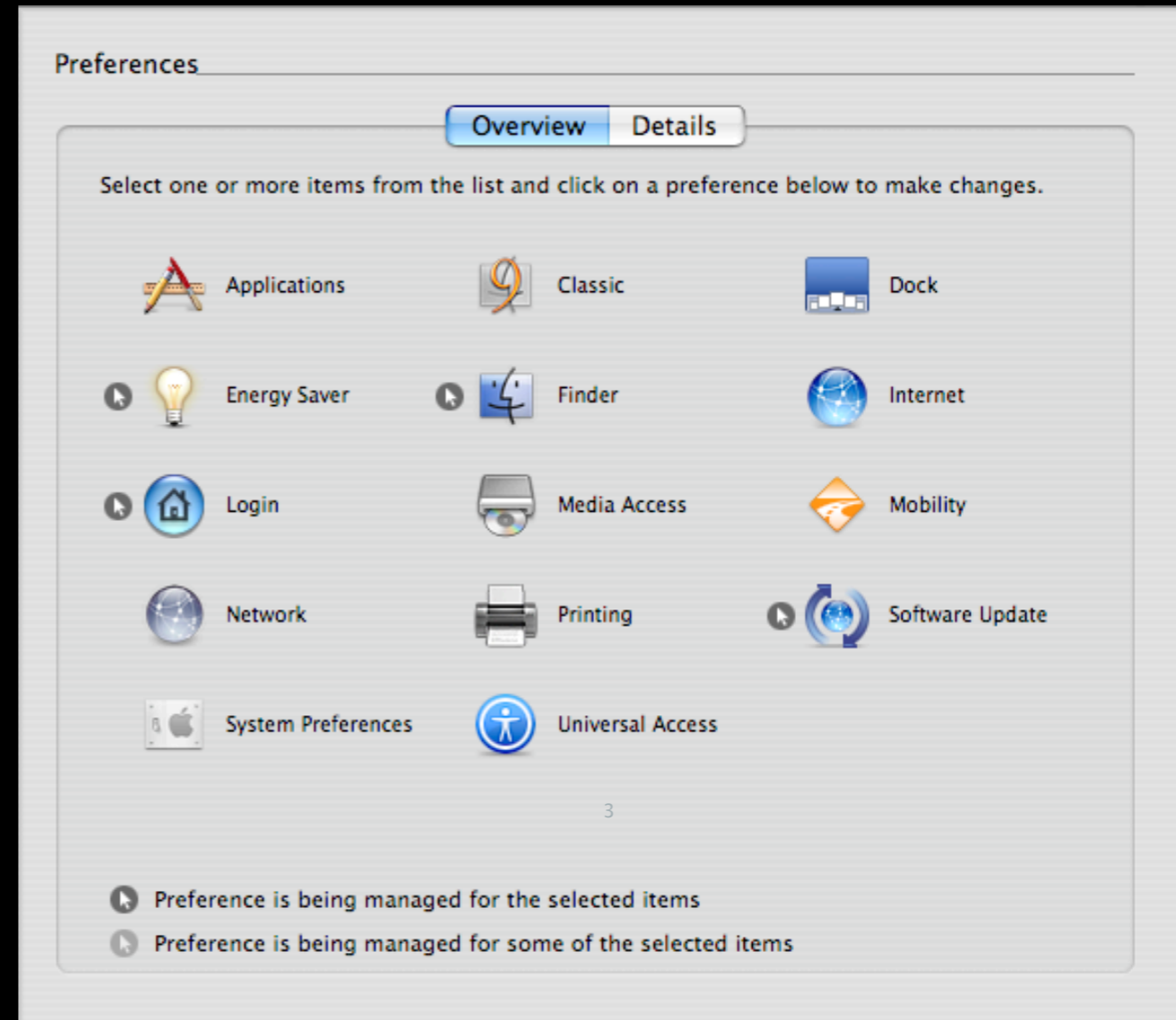
# Managing a Tiger Task – Usage Management

- Open Directory based
- LoginWindow controls
- Mobile Accounts with PHDs
- Preference Editor
- Remote Desktop v3



# Managed preferences

- Core OS Prefs
  - System settings
  - Applications
  - Media access
- Granular control
  - Login
  - Network
  - Mobility
- Extended control
  - Software Update



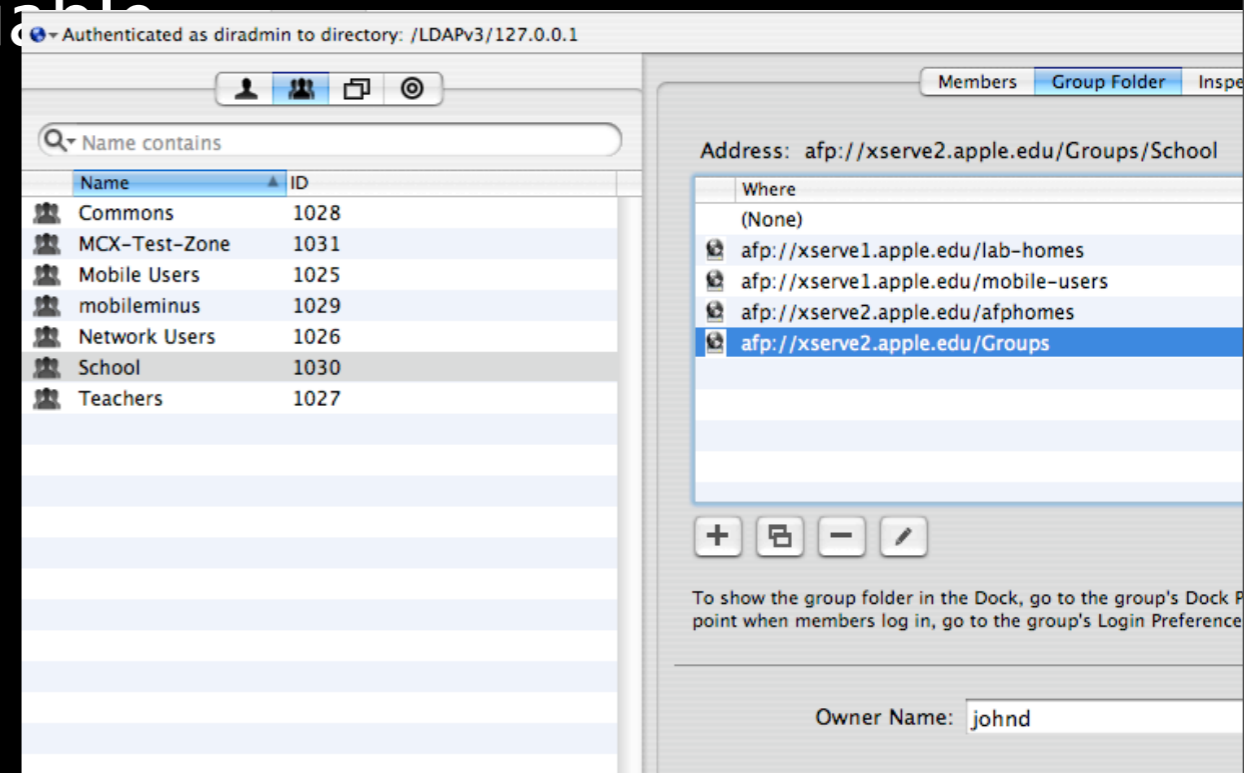
# Management is more than user passwords

- Account management
  - Computers managed by type and function
  - Users managed by curriculum or access level
  - Groups managed for workflow
- Workflow – don't wait until after you have deployed to figure it out
  - Common shared areas
  - Curriculum / Task specific sharepoints
  - Hand Out & Hand In capability
- Server load – disk space is cheap
  - ~150 concurrent users per dedicated network home server
  - ~300 concurrent users per dedicated portable home server
  - ~450 concurrent users per dedicated workgroup server



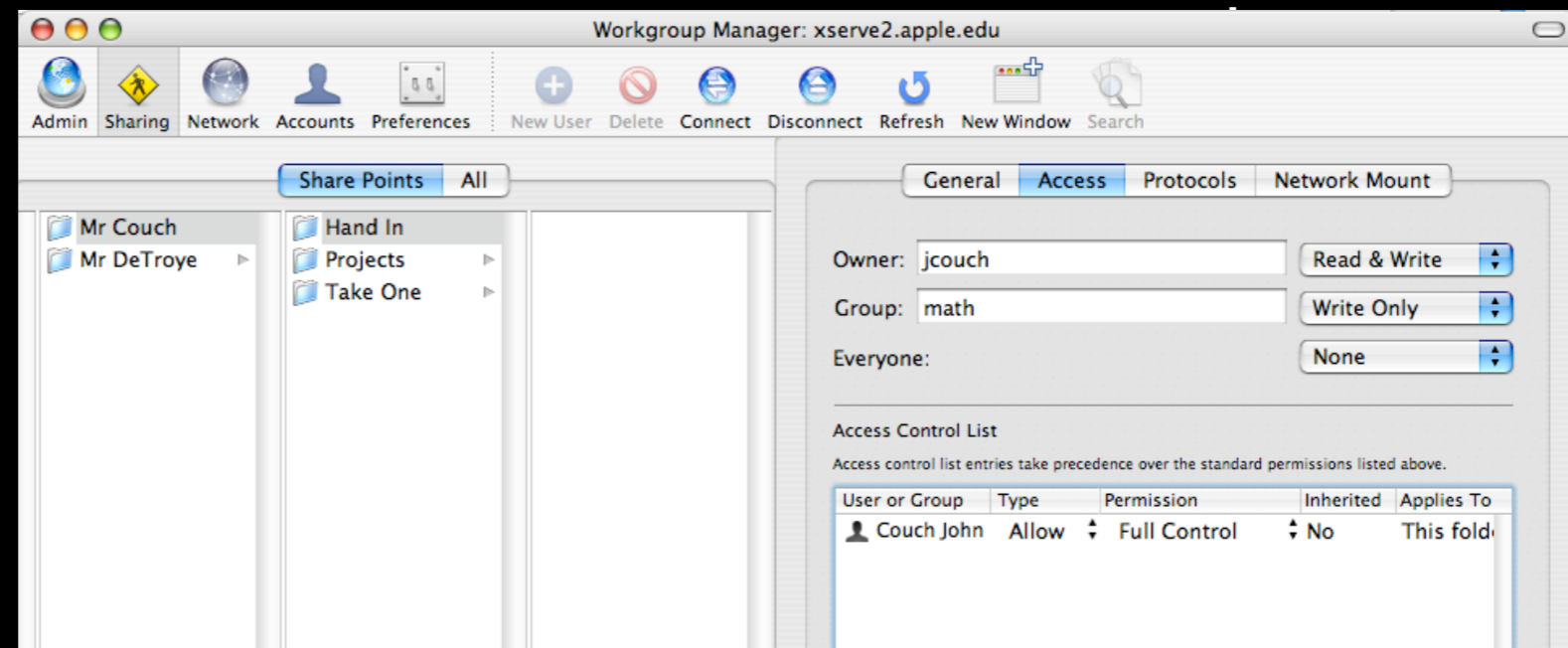
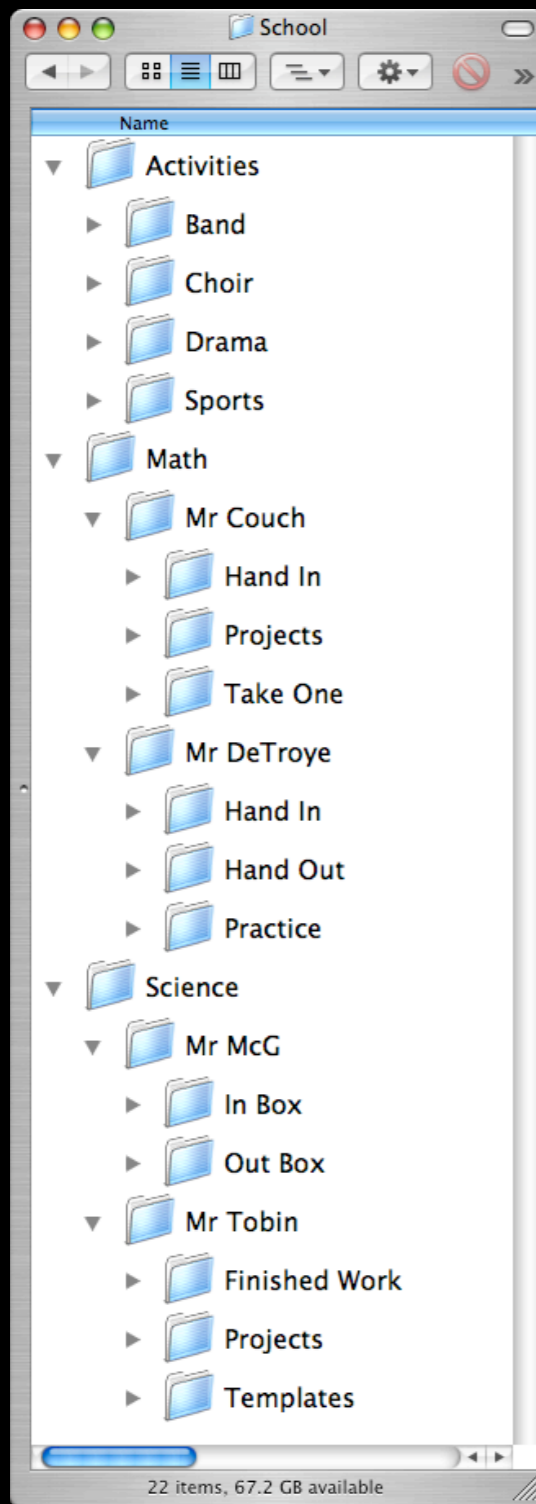
# The little understood (work)group folder

- Education demands electronic document workflow
- A group folder is not dependent on managed client
- Group folder(s) are infinitely modifiable
- Default group folder structure:
  - Documents
  - Library
  - Public (with Dropbox)
- Change it any way you desire!
  - Curriculum folders
  - Staff / admin / student folders
  - Special activities
  - Multiple sets belonging to different groups



# Group Folder redo

- Use ACL's to set special access
  - Read/write without delete
  - Multiple access Dropboxes
- Pull many groups together into one
  - Build a tiered structure
  - Create as complex or simple a



# User Account Management

## Three basic user account types

- Local account with local homedir
  - Pro—network independent, high performance
  - Con—difficult to manage en mass
- Network account with network homedir
  - Pro—easily managed remotely
  - Con—network traffic hog
- Mobile account
  - Pro—best of both worlds
  - Con—“rabbit effect”



# Mobile Accounts

- A mobile account is
  - A network based account cached as ...
  - A local user account with a local home directory
- A mobile account contains
  - Network based account information
  - Network based management settings
  - Locally created preferences (if allowed)
- Control and ownership
  - Directory admin owns the existence of the account
  - Local admin owns the existence of the working homedir
- Mobile accounts are used in 1:1 deployments but...





# Mobile Accounts Are More Than 1:1's

- Use mobile accounts when
  - Load on home directory is critical
  - System is often user's only computer
  - Network traffic needs to be minimized
  - Computer is often off-net
- Mobile accounts can work in
  - Staff/faculty desktops
  - Temporary use systems
  - NetBoot environments
  - Shared computer labs (training / common use)



# Directory Information

## Account data sync

Basic | Advanced | Groups | Home | Mail | Print Quota | Info | Windows | Inspector

Filter:  Record Size: 4.70 KB

Name	Size	Value
AppleMetaNodeLocation	17 bytes	/LDAPv3/127.0.0.1
▶ AuthenticationAuthority(2)	837 bytes	;ApplePasswordServer;
GeneratedUID	36 bytes	F82066D6-E152-4C3F-91A2-
HomeDirectory	79 bytes	<home_dir> <url>afp://
Keywords	7 bytes	primary
LastName	2 bytes	99
MCXFlags	283 bytes	<?xml version="1.0" encoding="UTF-
▶ MCXSettings(2)	3.29 KB	<?xml version="1.0" encoding="UTF-
NFSHomeDirectory	42 bytes	/Network/Servers/pserve2.local/Users
Password	8 bytes	*****
Picture	28 bytes	/Library/UserPics/johnd.tiff
PrimaryGroupID	2 bytes	20
RealName	12 bytes	DeTroye John
▶ RecordName(2)	17 bytes	johnd
RecordType	23 bytes	dsRecTypeStandard:Users

Options... Edit... New Value... New Attribute...

Network Directory (OpenLDAP)

Property	Value(s)
original_node_name	/LDAPv3/pserve1.apple.edu
▶ name	(johnd, DeTroye John)
mcx_flags	<?xml version="1.0" encoding="UTF...
home	/Users/johnd
▶ original_authentication_authority	(;ApplePasswordServer;0x427ed4200...
authentication_authority	;LocalCachedUser;/LDAPv3/pserve1...
passwd	*****
lastname	99
_writers_picture	johnd
realname	DeTroye John
uid	10125
original_home	/Network/Servers/pserve2.local/User...
▶ preserved_attributes	(dsAttrTypeStandard:AuthenticationA...
shell	/bin/bash
generateduid	F82066D6-E152-4C3F-91A2-B018E...
gid	20
▶ mcx_settings	(<?xml version="1.0" encoding="UTF...
original_home_loc	<home_dir> <url>afp://pserve2.appl...
copy_timestamp	2005-05-22T20:43:41Z
picture	/Library/UserPics/johnd.tiff

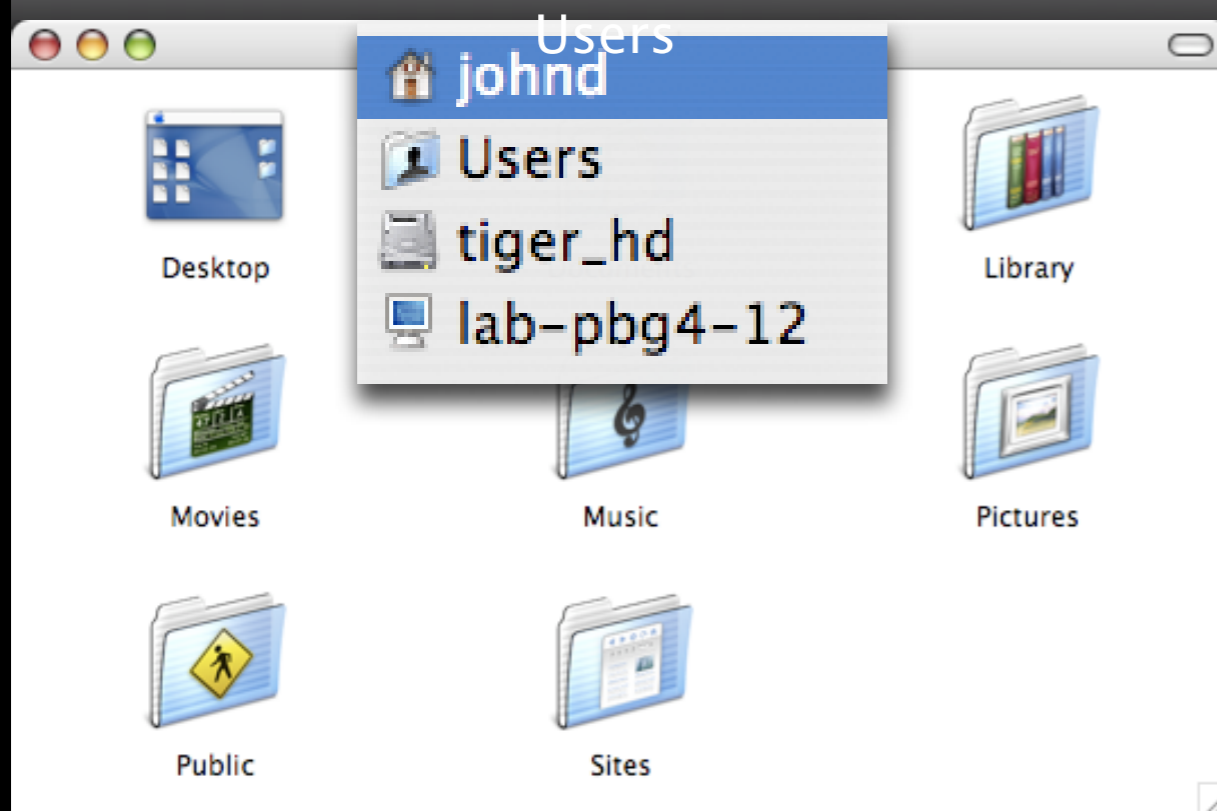
Local Directory (NetInfo)



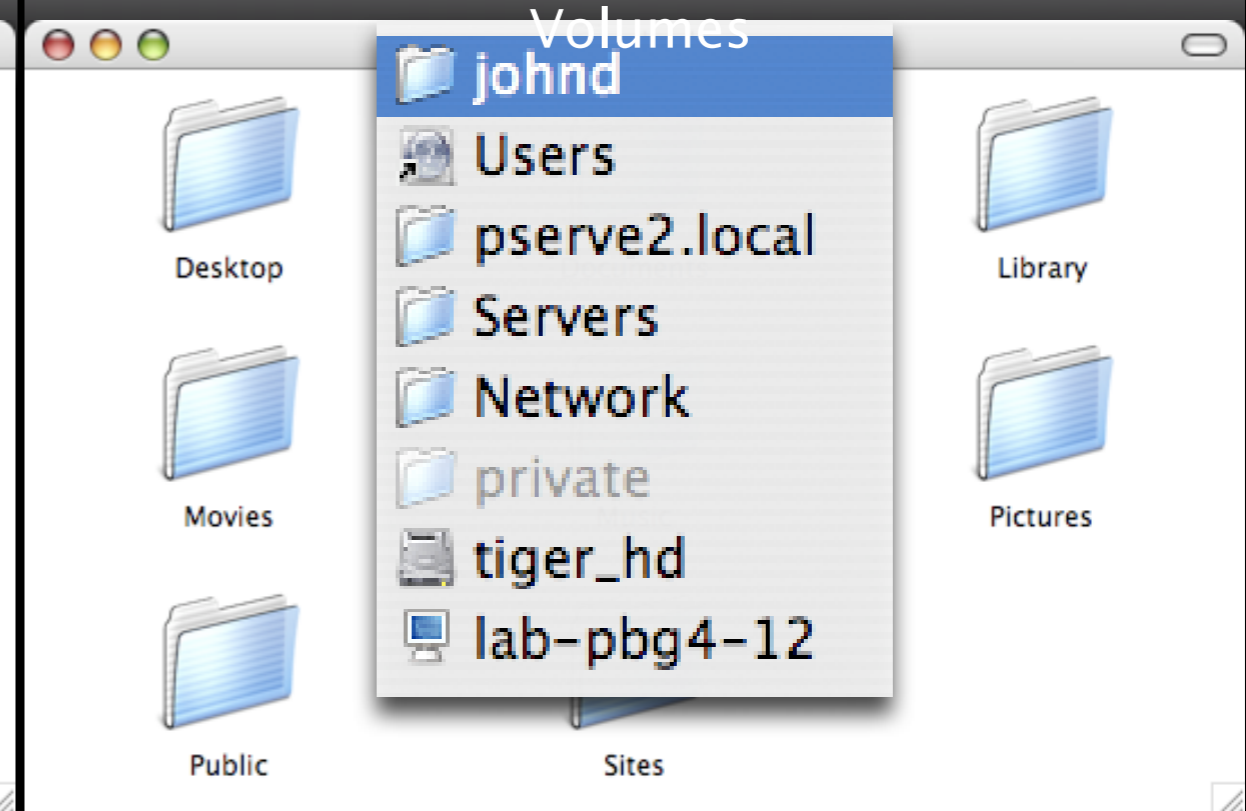
# Mobile Account Home Directories

## Local and Network home directories

User's local home is created in /



User's Network home is mounted in /



# Portable Home Directories

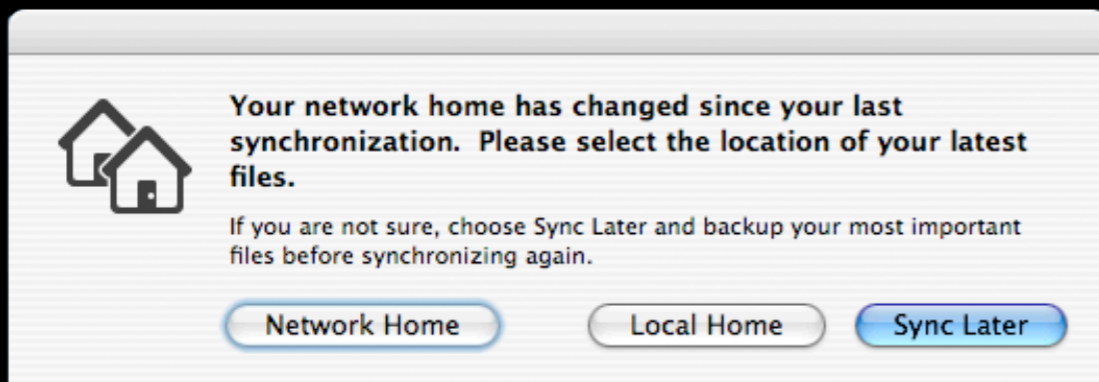
Tiger feature – not in Panther

- Mobile account limitation under Panther
  - Account sync—not document sync
- Customer requirement
  - “I need my users’ work preserved / backed up / maintained...”
- Mobile account with Portable Home Directory
  - Establish file level synchronization between local and network homedir
  - Allow for filtering of undesirable files / folders
  - Make it flexible—login/logout and/or background sync
  - Allow for on-demand sync



# PHD Logic

2-way sync using same engine as iDisk sync

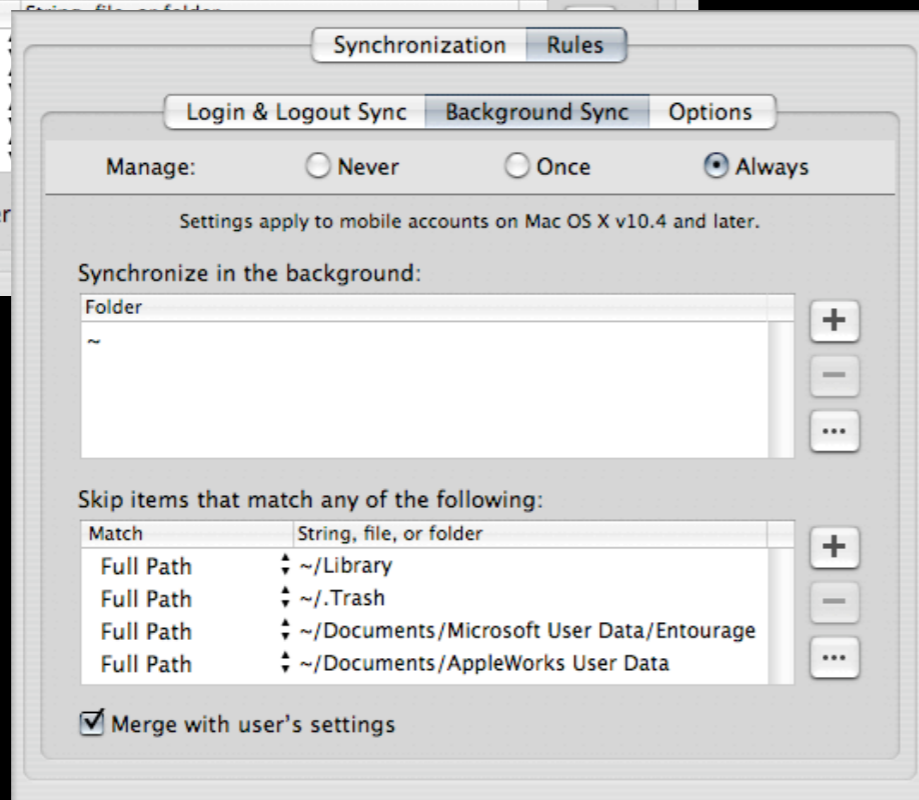
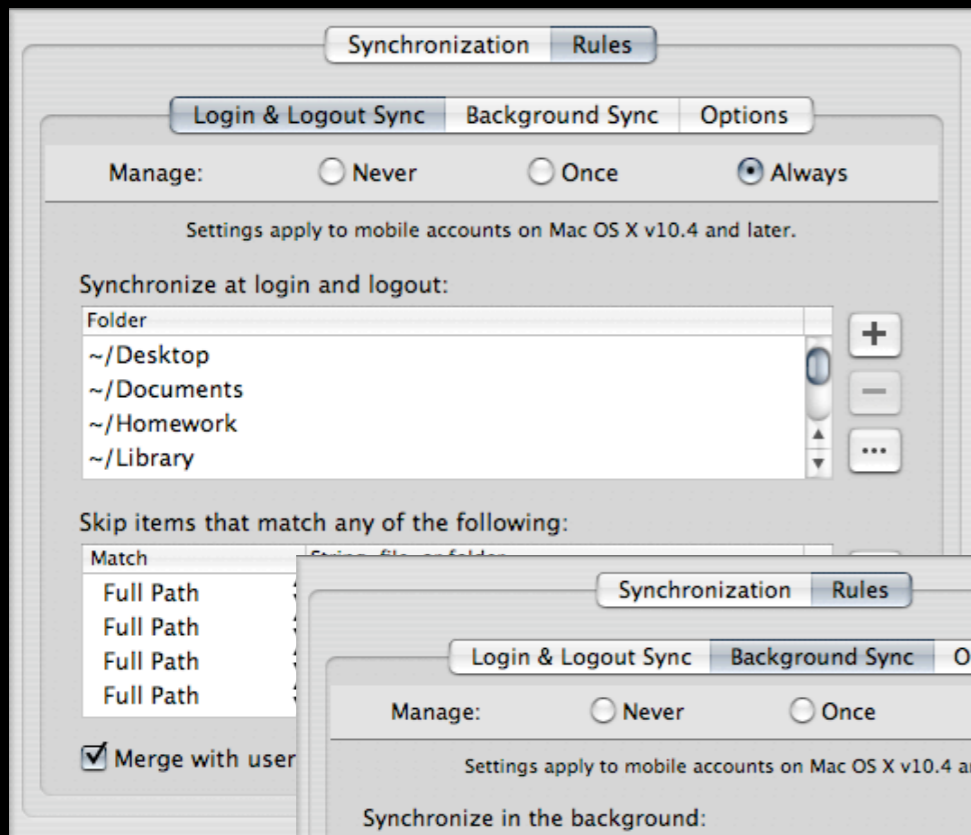


- Create a db of all files in user's home directory at both locations
- At sync, compare file datetime stamps
- Synchronize allowed files to maintain most current items
- Provide for key out of bounds cases
  - User changes local system



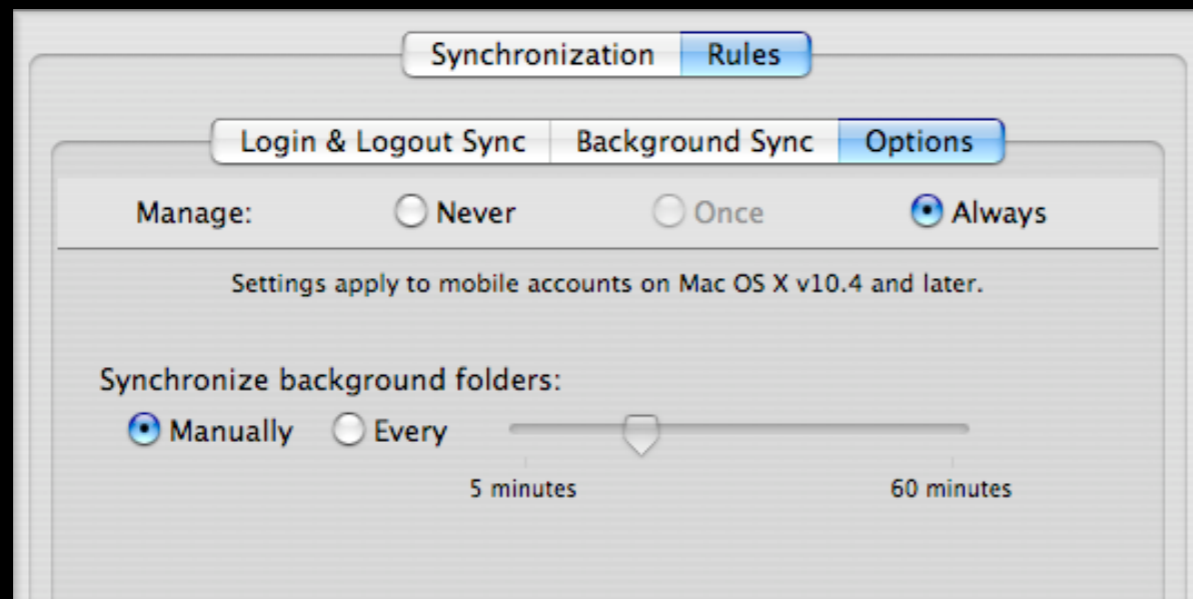
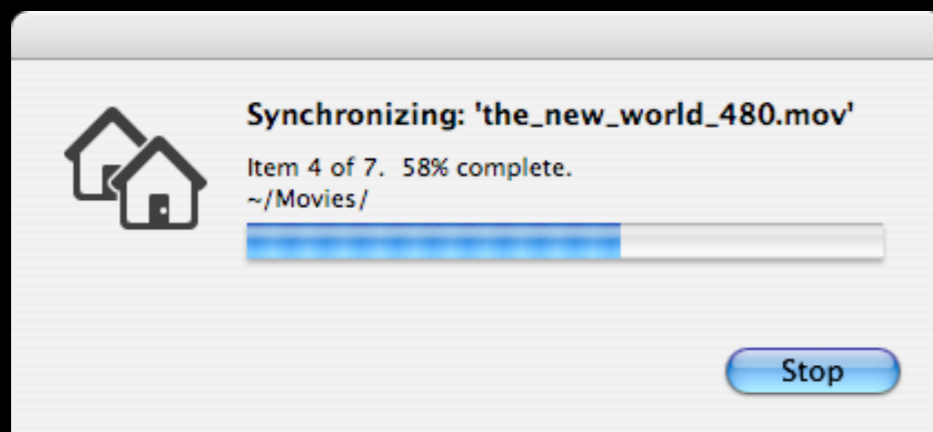
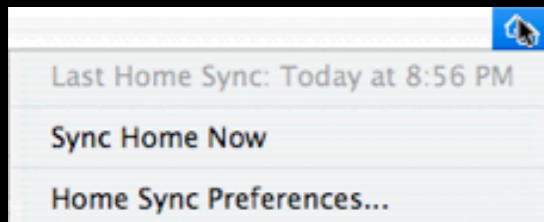
# PHD Options

- Folder based sync with filters
- Login / Logout sync
- Background (periodic) sync
- Supports rule-based filters
  - Path names (folders)
  - File names (files)
  - Case sensitive filtering  
.MP3 ≠ .mp3



# Optional Sync

- Applies to background sync
- Option to set for manual or periodic syncing
- Choose based on user behavior, network, and time allowance



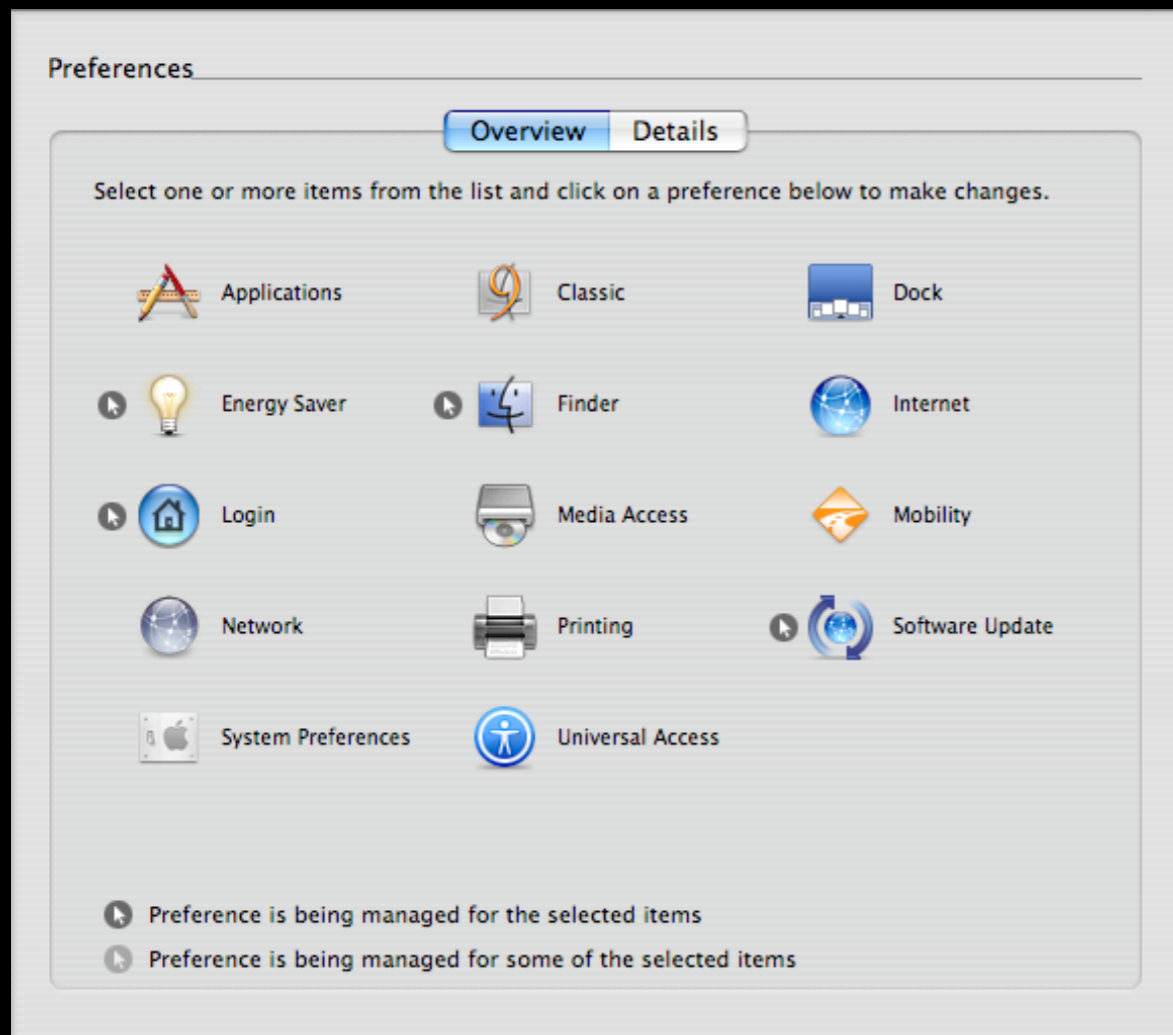
# Sync Policies and PHDs

- Login/Logout sync needed to set up ~/Library
  - User's preferences, bookmarks, Mail
  - iPhoto and iTunes
    - Music and Pictures are outside ~/Library
    - Album and Playlist definitions are inside ~/Library
- Sync process can become network intensive
- Workflow should determine filter and folder settings
- Multiple sync settings can be created by using group / computer accounts
  - Sync only certain folders when users are in restricted areas
  - Sync everything in more open settings
  - Manual sync when background sync might interfere with application





# Mobile Accounts and Management

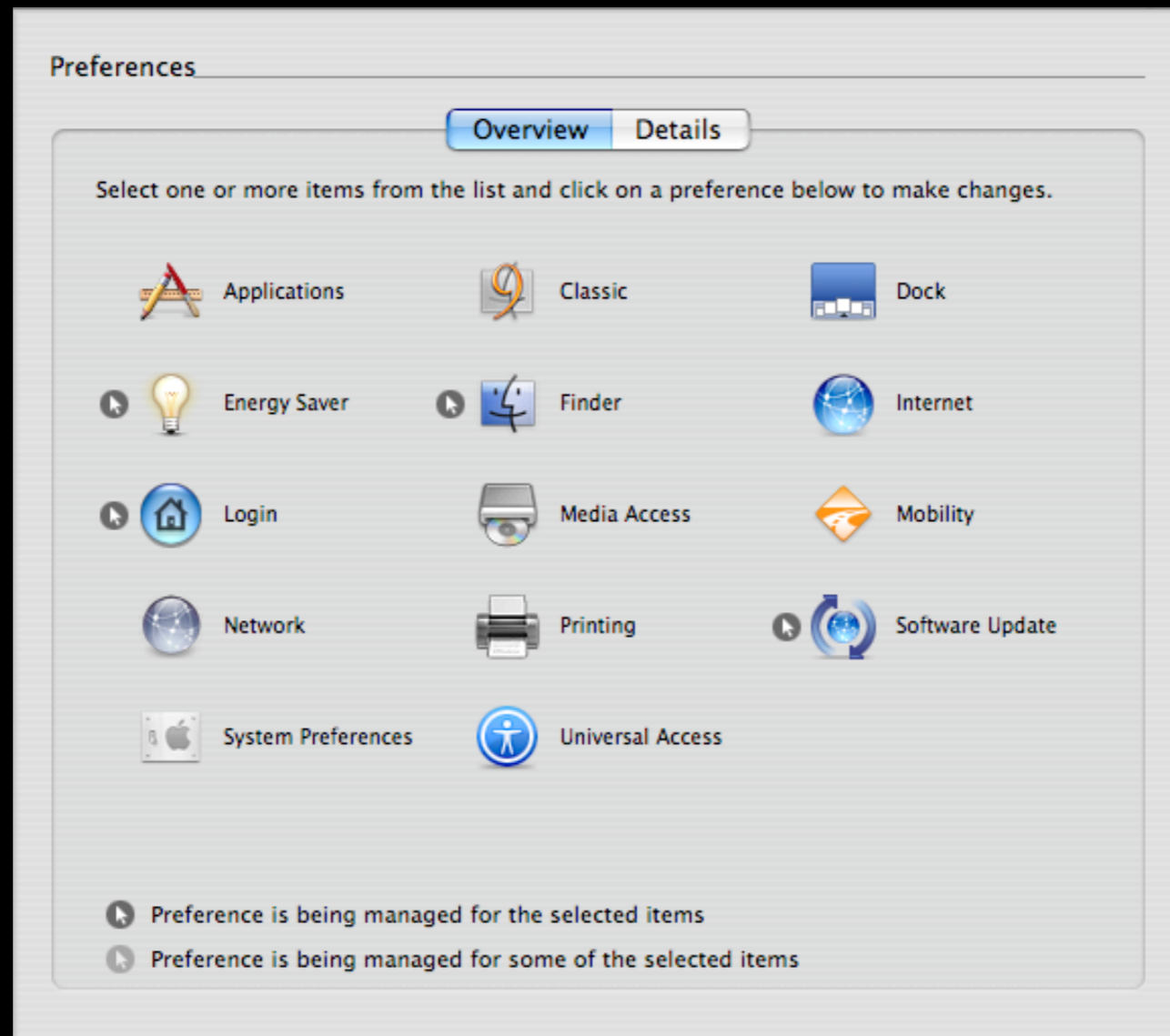


- Mobile accounts are established using managed client settings
- Using network based management extends flexibility of mobile account



# Attention to Detail(s)

## Managing non-System Preferences



# Preference Editor

## Granular control

Safari (com.apple.Safari)

New Key Delete Set Default Delete Unmatched

Name	Type	Value
▶ Once	dictionary	empty
⚠ ▼ Often	dictionary	53 items
ActivitiesStartExpanded	boolean	true
AddressBarIncludesHome	boolean	true
AddressBarIncludesTextSizing	boolean	true
AddressBarPreferencesWereConverted	boolean	true
Allow JavaScript to Open Windows Automatically	boolean	false
Always Show Tab Bar	boolean	true
AppleNavServices:PutFile:0:Disclosure	data	<01>
AppleNavServices:PutFile:0:ExtensionHidden	data	<01>
AppleNavServices:PutFile:0:HomeDirectoryPath	string	file://~/Desktop/
AppleNavServices:PutFile:0:Path	string	file://localhost/Users/johnd/Desktop/
AppleNavServices:PutFile:0:Position	data	<01d70232 >
AppleNavServices:PutFile:0:Size	data	<00000000 00870230 >
AutoFill From Address Book	boolean	false
AutoFill Miscellaneous Forms	boolean	false
Bookmarks Collections Include Address Book	boolean	false
Bookmarks Collections Include Bonjour	boolean	false

Safari preferences

⚠ means this item does not match the preference manifest

Done Revert Apply Now



# Preference Manifest

## Built-in management

Safari (com.apple.Safari)

New Key Delete

Name	Type	Value
▶ Once	dictionary	empty
▶ Often	dictionary	empty
▼ Always	dictionary	1 item
Allow JavaScript to Open Windo...	boolean	true

FALSE to block pop-up windows

means this item does not match the preference manifest

Done

- Contents of New Windows
- Downloads Clearing Policy
- Open Safe Downloads Automatically
- Open External Links in Existing Window
- Default Font
- Default Fixed-width Font
- Default Fixed-width Font Size
- Display Images
- Default Text Encoding
- Bookmarks Bar Includes Address Book
- Bookmarks Bar Includes Bonjour
- Bookmarks Menu Includes Bookmarks Bar
- Bookmarks Menu Includes Address Book
- Bookmarks Menu Includes Bonjour
- Bookmarks Collections Include Address Book
- Bookmarks Collections Include Bonjour
- Tabbed Browsing Enabled**
- New Tabs are Selected
- Always Show Tab Bar
- AutoFill From Address Book
- AutoFill Passwords
- AutoFill Miscellaneous Forms
- Plug-ins Enabled
- Java Enabled
- JavaScript Enabled
- Allow JavaScript to Open Windows Automatically
- Ask Before Submitting Insecure Forms
- Minimum Font Size
- Tab to Links
- Enable User Style Sheet
- User Style Sheet Location
- Print Backgrounds
- Print Headers and Footers

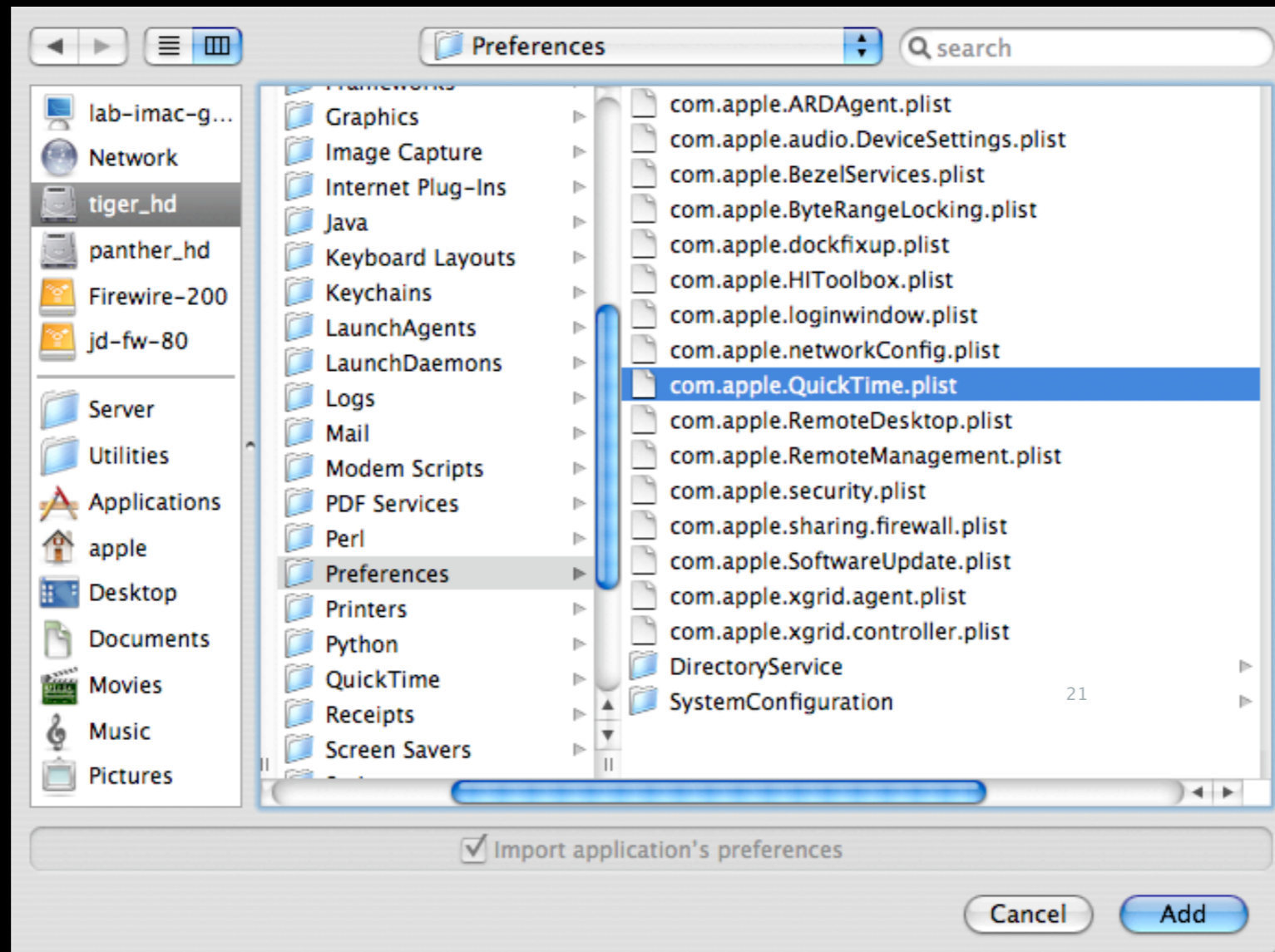
✓ New Item

Edit



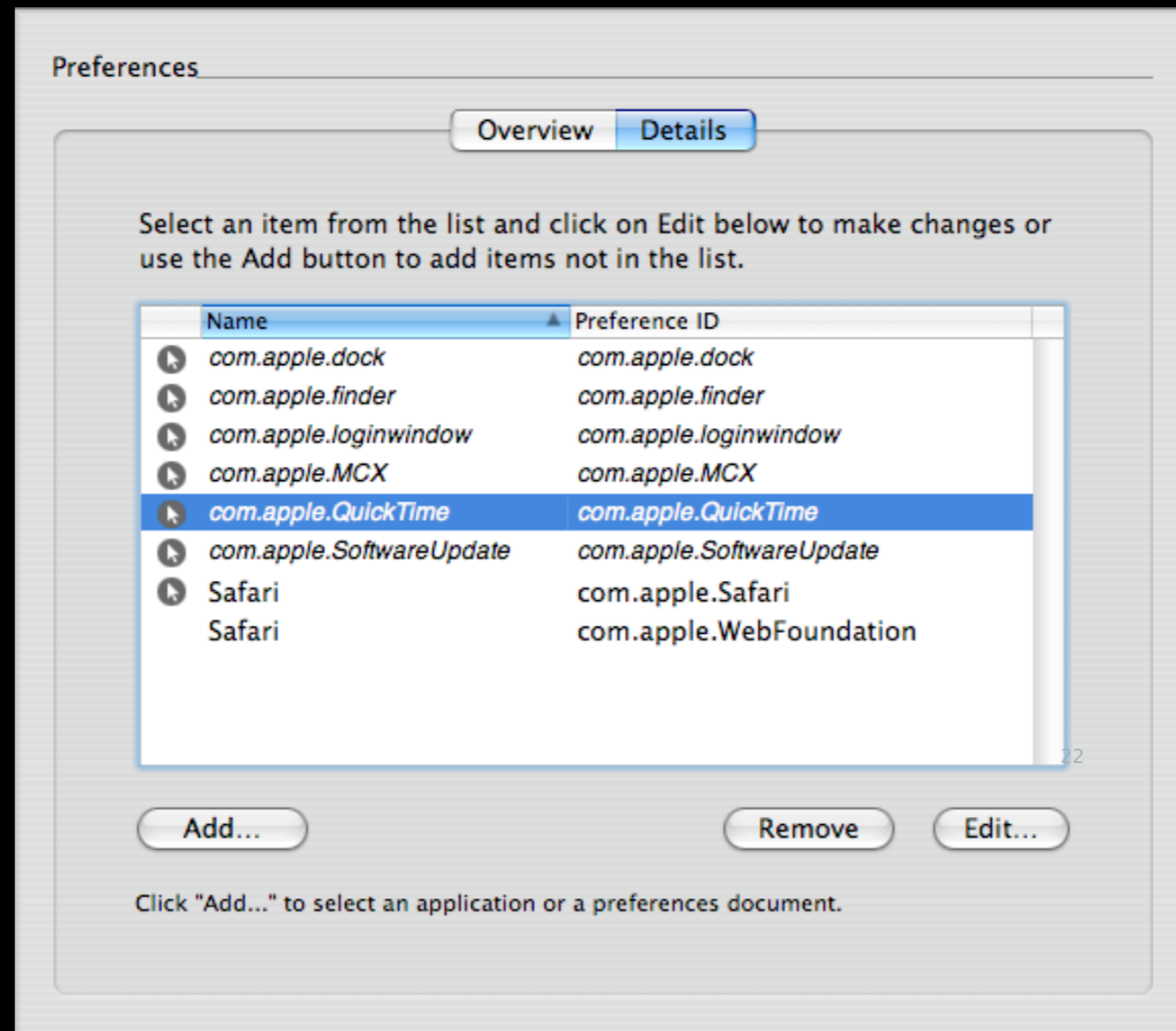
# Adding normal preferences

## Using admin defined preferences



# QTPro—For Everyone

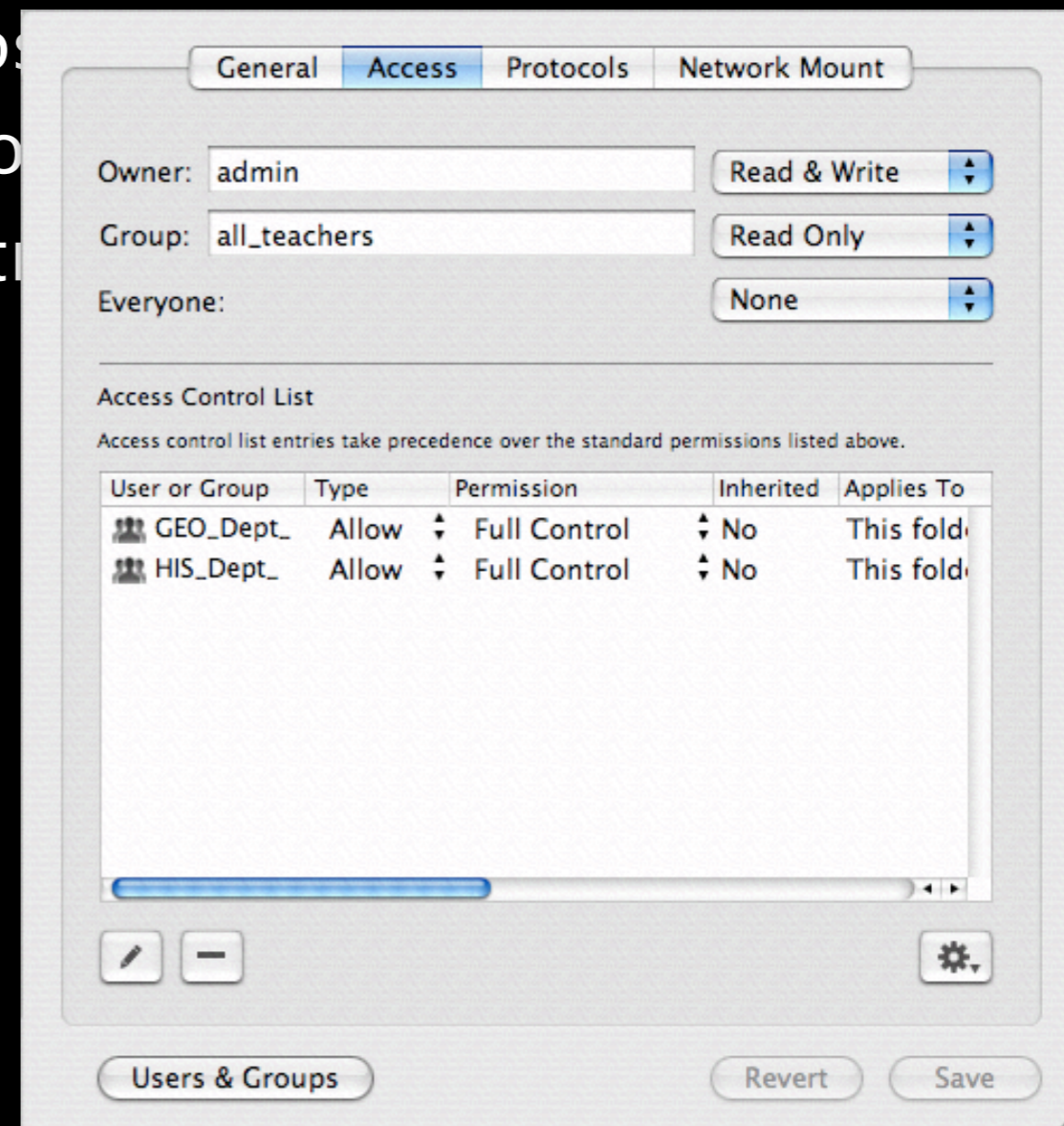
All QT prefs applied—incl. serial number



# Access Control Lists (ACLs)

A kazillion ways to configure access to files / folders

- Provides an extended set of permissions for a file or folder
- Allows you to set permissions for multiple users and groups
  - simulates them being owners or groups
- Groups can be nested within other groups
- Contain a series of Access Control Entries
  - an ordered list of permissions
- Work in addition to the standard POSIX permissions



# Service Access Control Lists (SACLs)

Allow you to specify which users and groups have access to services

- AFP
- FTP
- iChat
- Login Window
- Mail
- SSH
- VPN
- Web
- Weblog
- Windows
- Xgrid

Another layer of control on top of POSIX and ACLs

