Managing Tigers

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

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

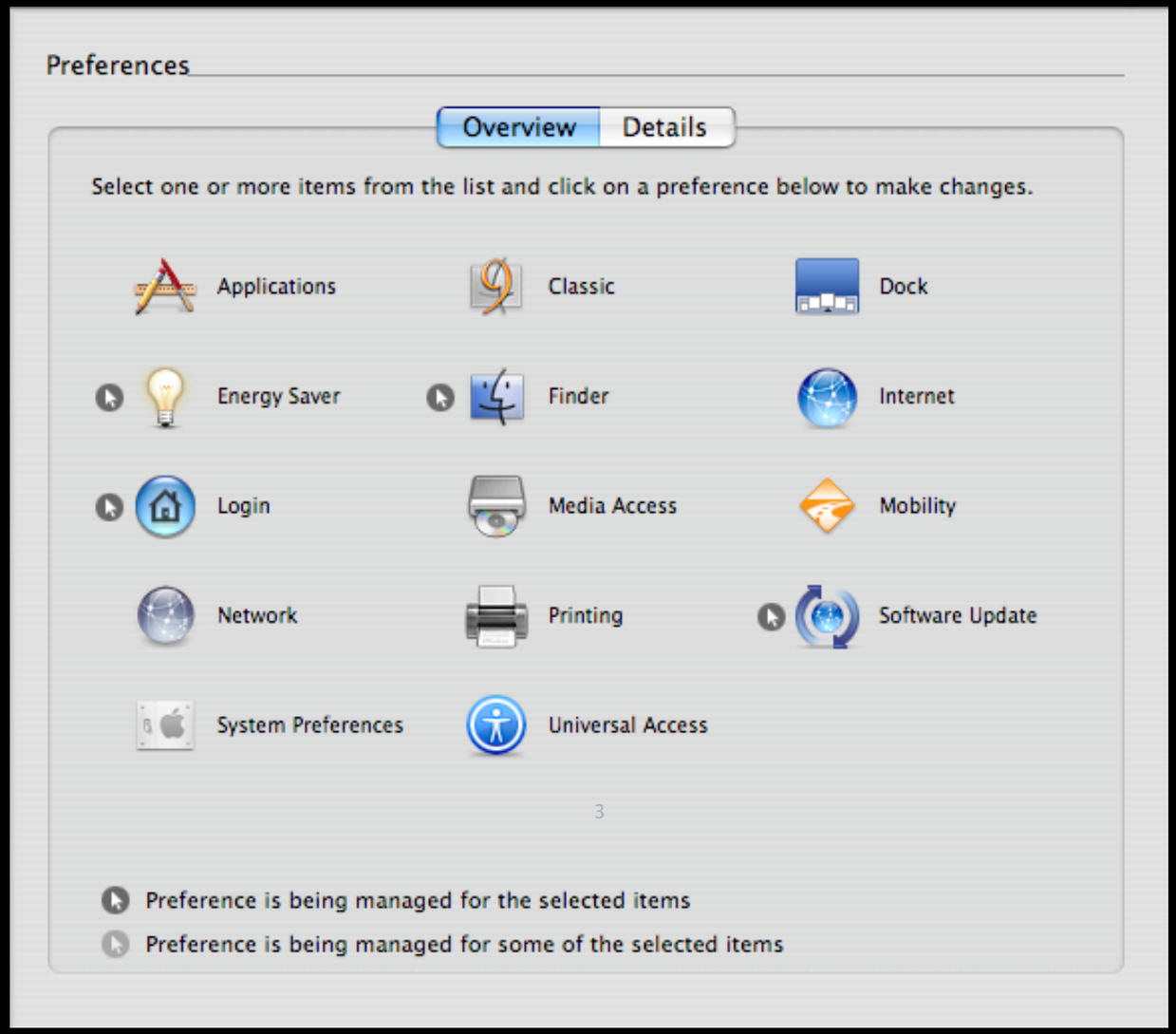
Managing a Tiger

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 conrol
  - Software Update

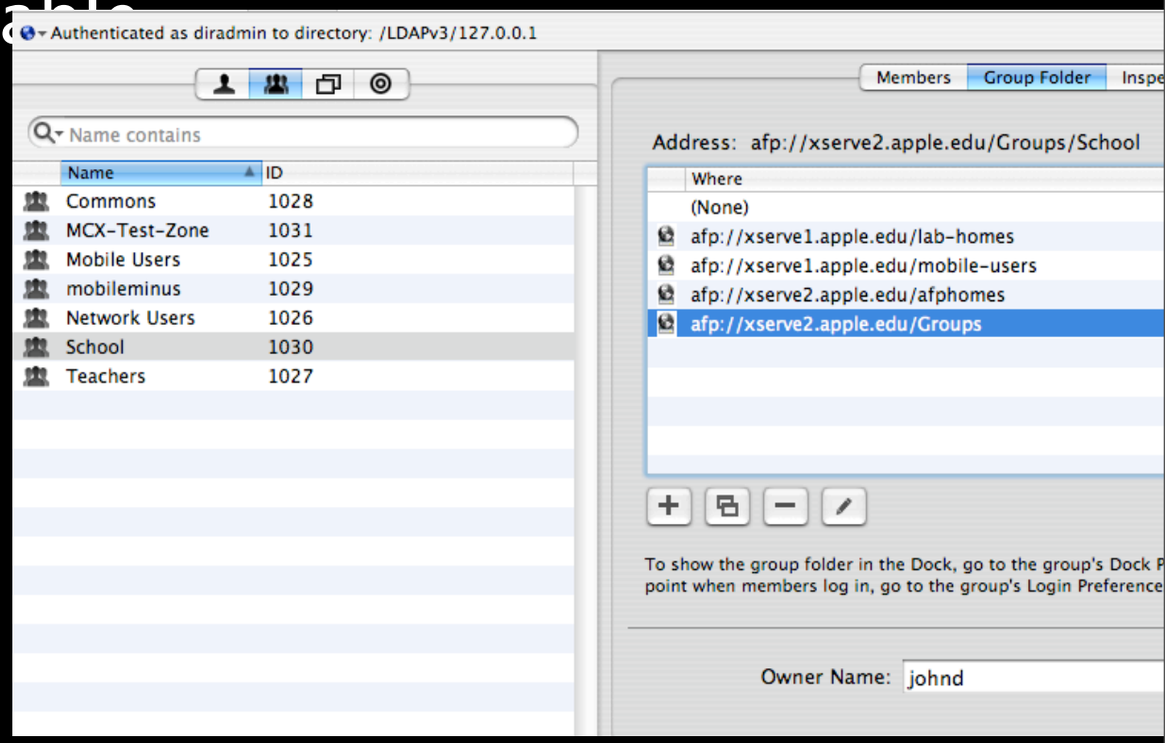


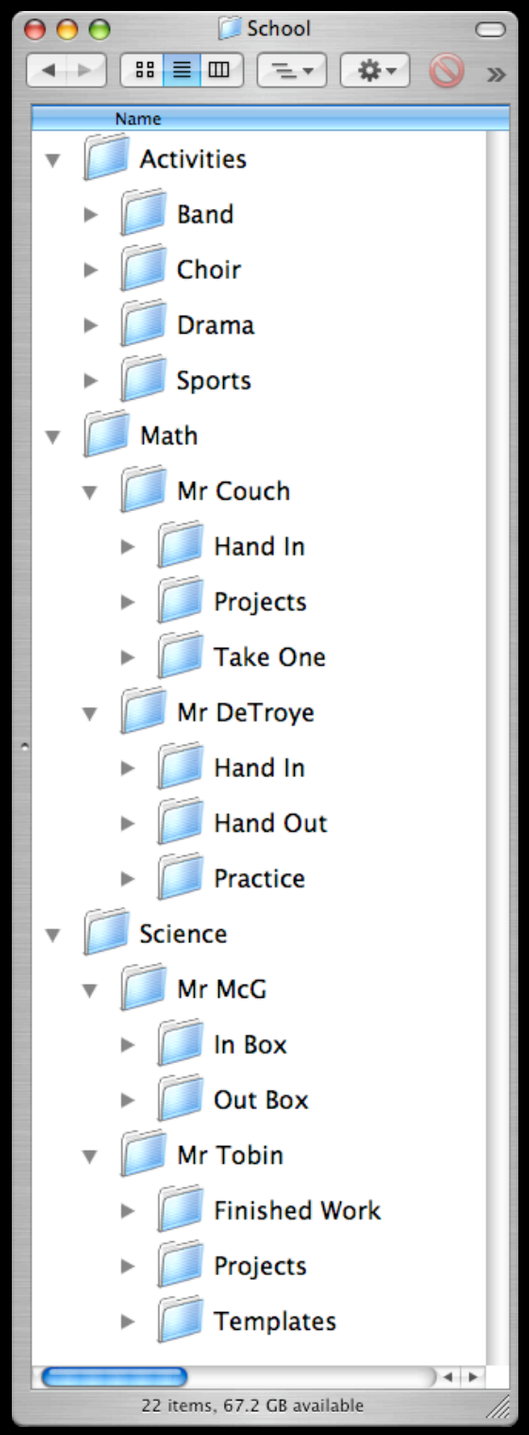
Management is more than user passwords

- 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

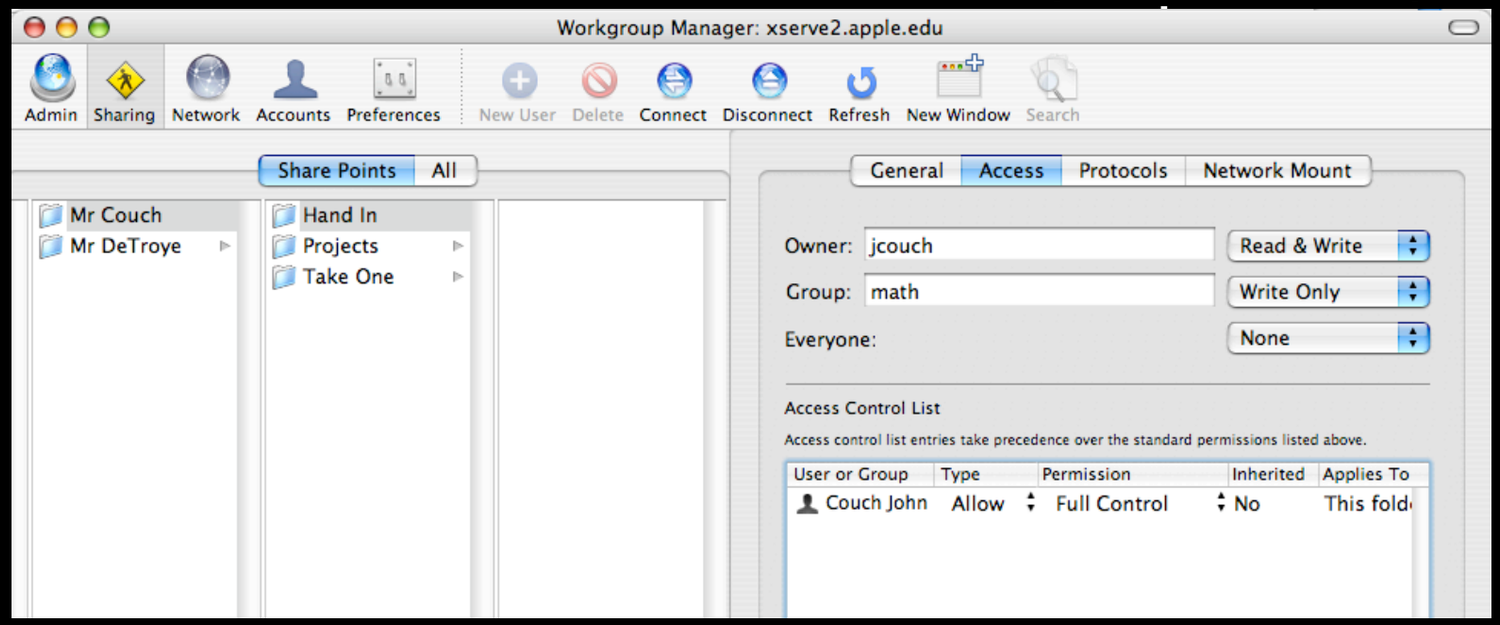
- Education demands electronic document workflow
- A group folder is not dependent on managed client
- Group folder(s) are infinitely modifiable
- Default group folder structure:
  - Documents
  - Library
  - Public (with Dropbox)
- Change it any way you desire!
  - Curriculum folders
  - Staff / admin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

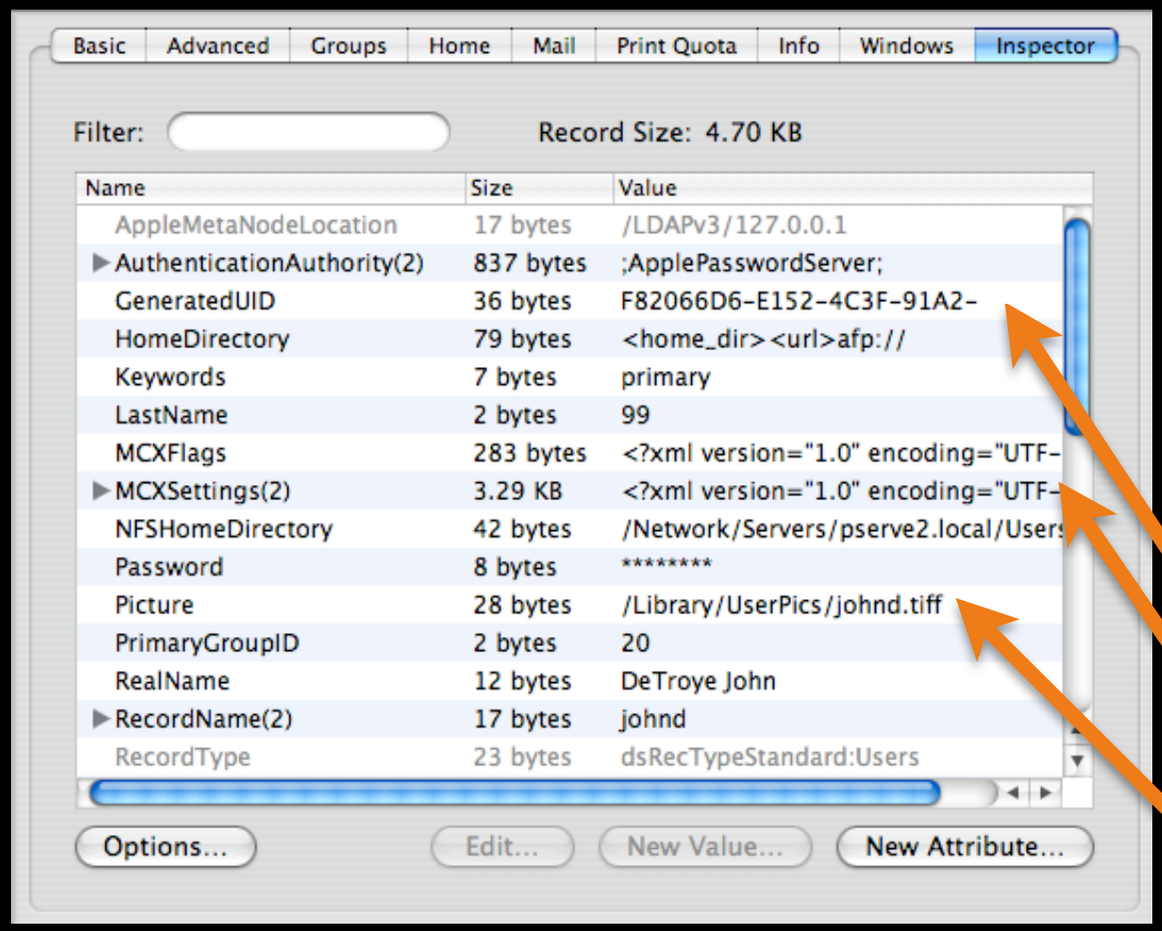
- A mobile account is
  - A network based account cached as ...
  - A local user account with a local home directory
- A mobile account contains
  - Network based account information
  - Network based management settings
  - Locally created preferences (if allowed)
- Control and ownership
  - Directory 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

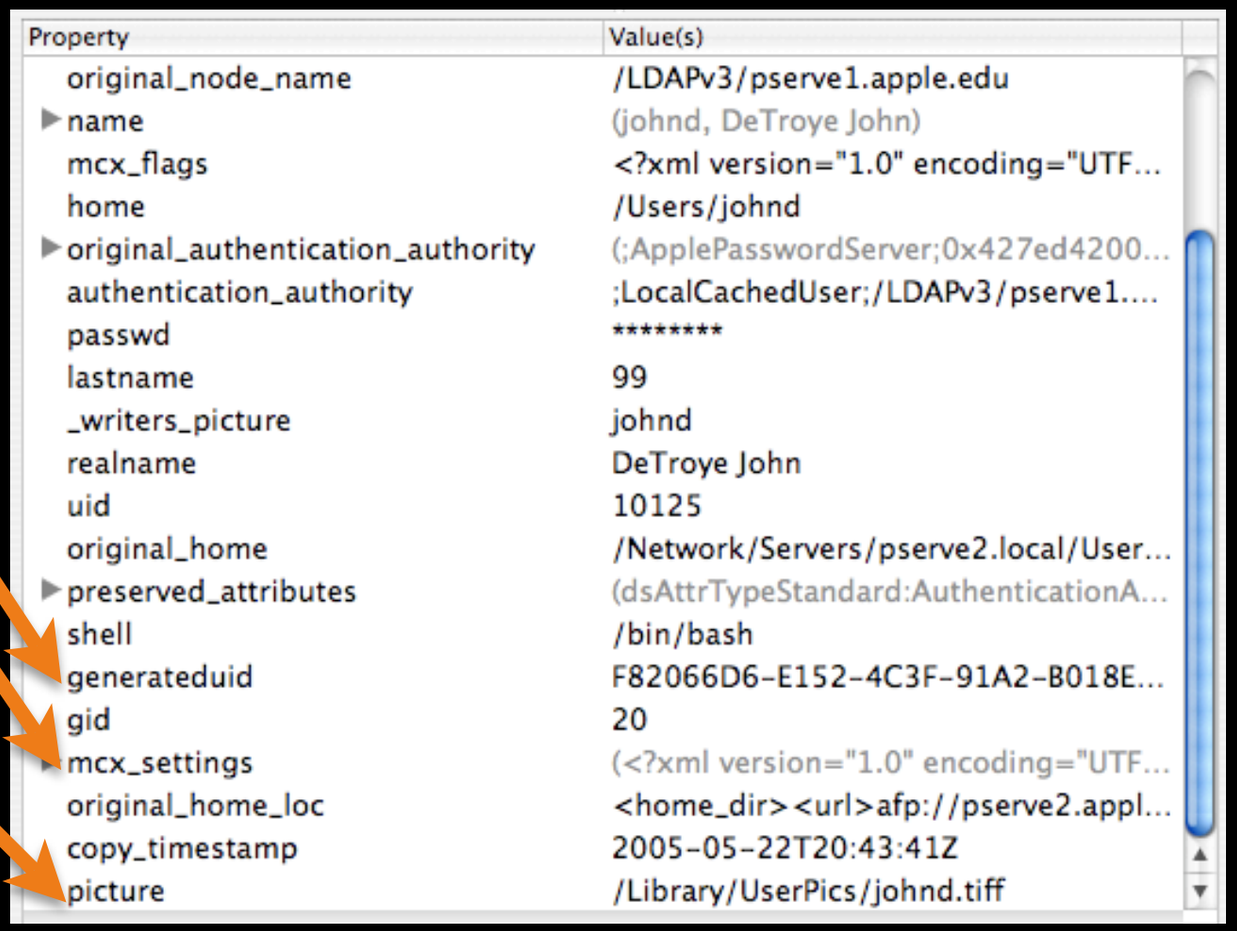
- Use mobile accounts when
  - Load on home directory is critical
  - System is often user's only computer
  - Network traffic needs to be minimized
  - Computer is often off-net
- Mobile accounts can work in
  - Staff/faculty desktops
  - Temporary use systems
  - NetBoot environments
  - Shared computer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

Directory Information

Account data sync



Network Directory (OpenLDAP)

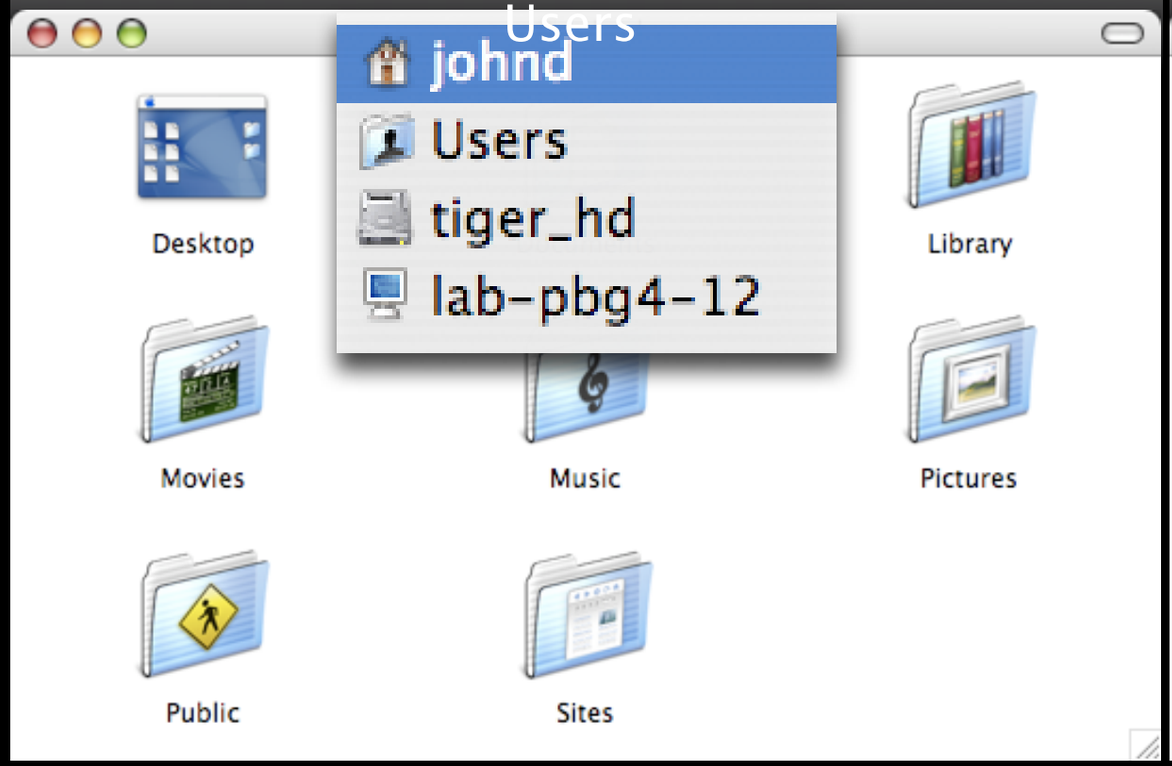


Local Directory (NetInfo)

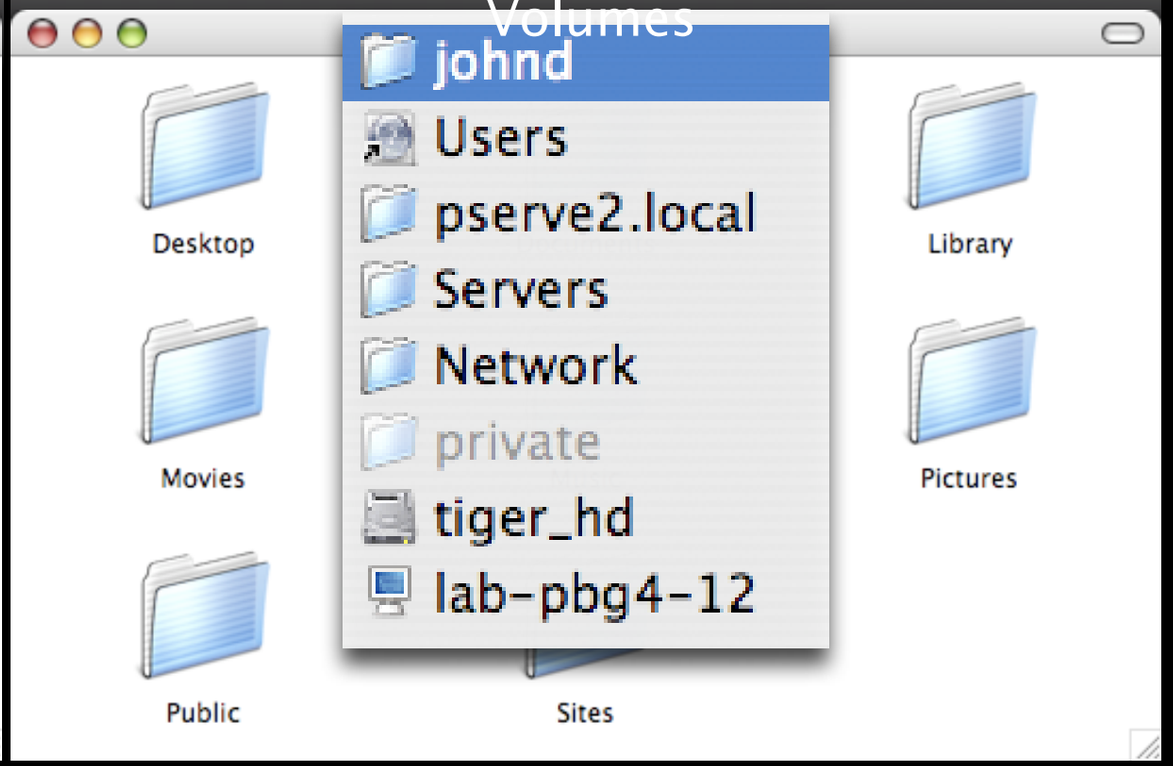
Mobile Account Home Directories

Local and Network home directories

User's local home is created in /Users



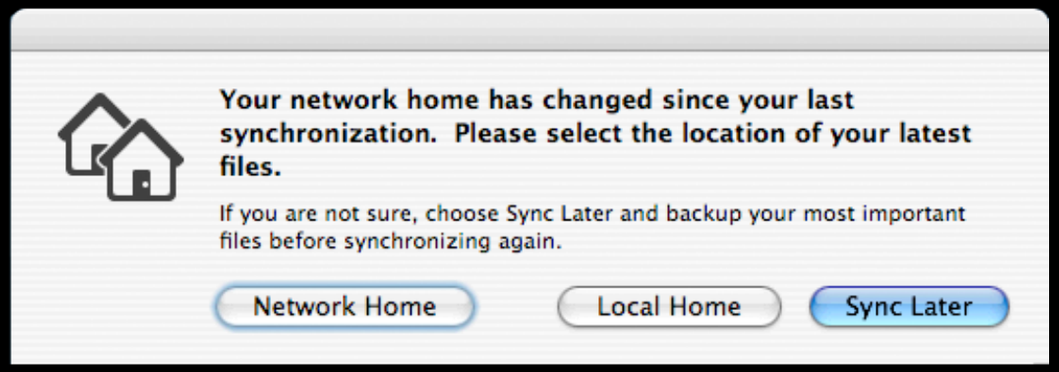
User's Network home is mounted in /Volumes



Portable Home Directories

Tiger feature – not in Panther

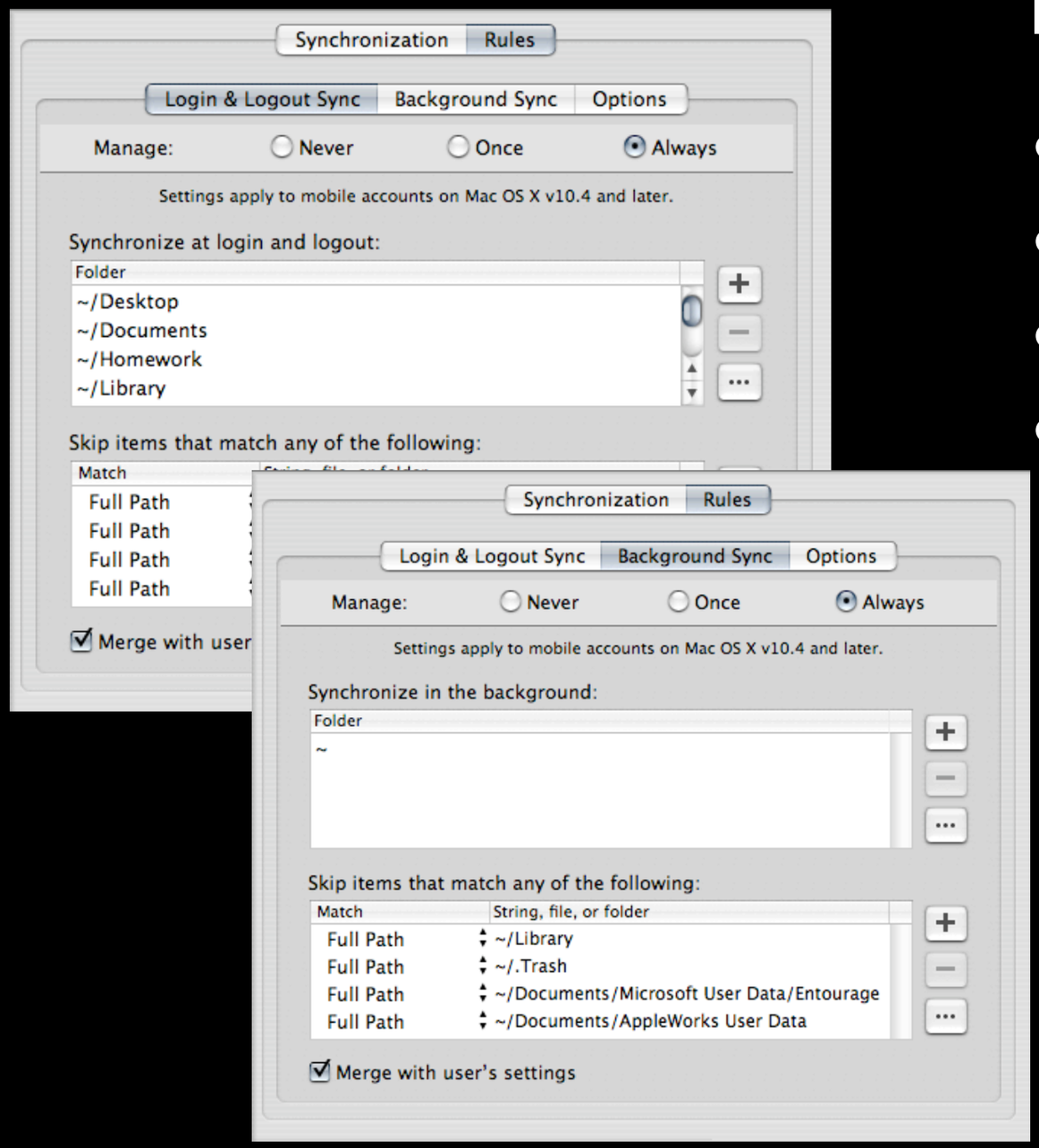
- Mobile account limitation under Panther
  - Account sync—not document sync
- Customer requirement
  - "I need my users' work preserved / backed up / maintained…"
- Mobile account with Portable Home Directory
  - Establish file level synchronization between local and network homedir
  - Allow for filtering 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

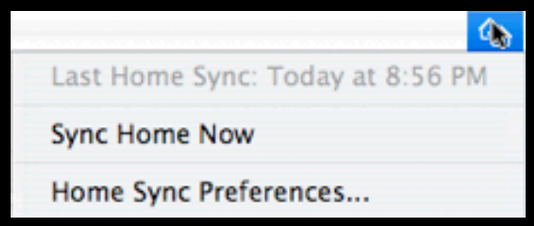
- Create a db of all files in user's home directory at both locations
- At sync, compare file datetime stamps
- Synchronize allowed files to maintain most current items
- Provide for key out of bounds cases
  - User changes local system

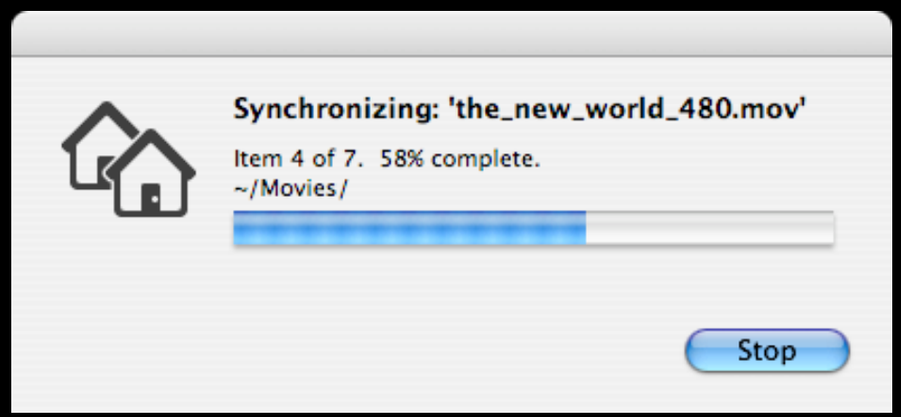


PHD Options

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

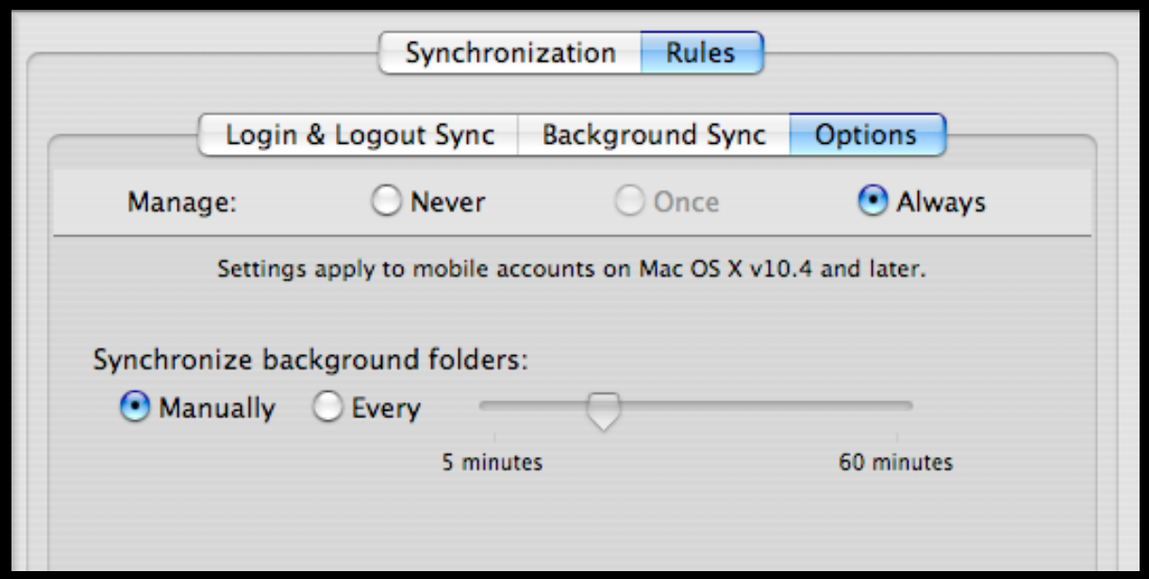
  .MP3 ≠ .mp3





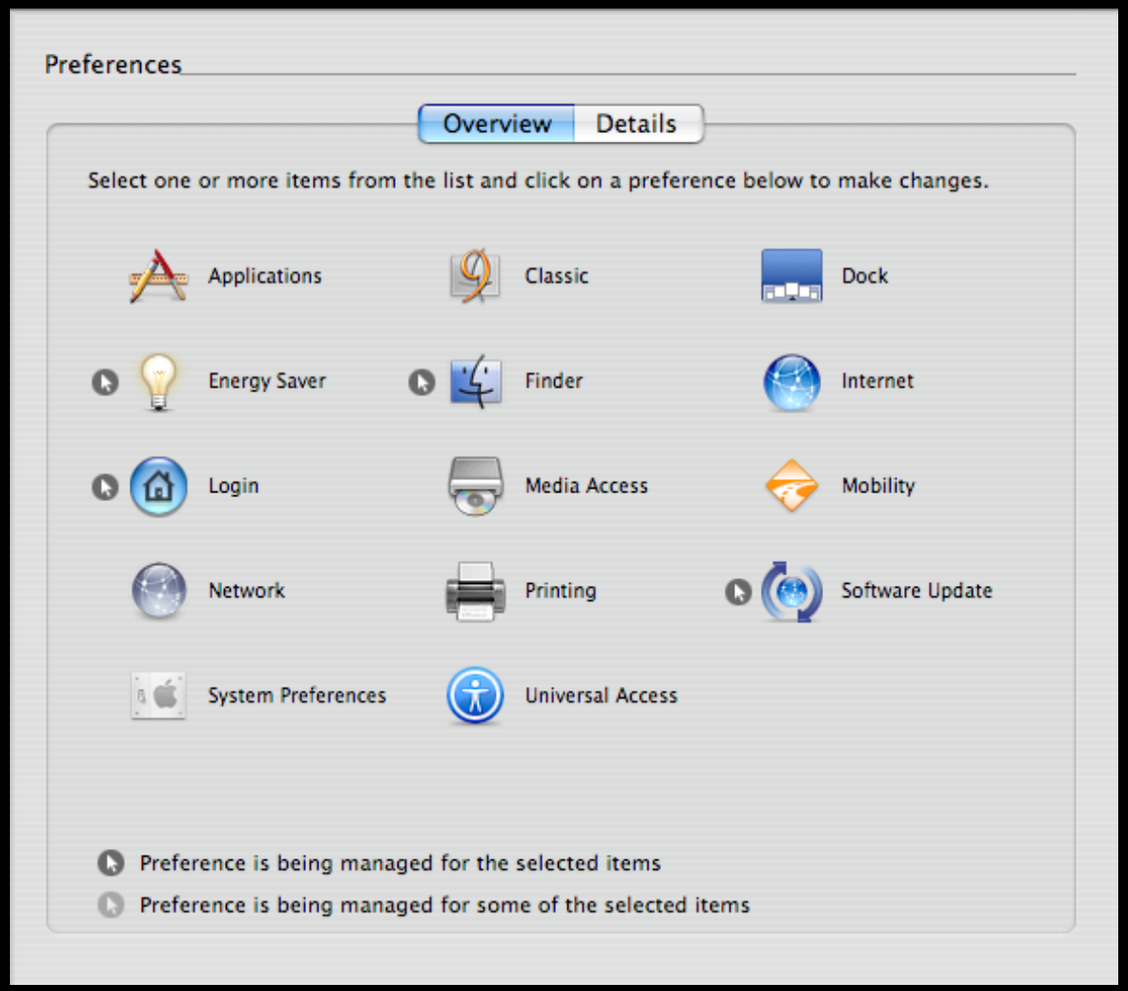
Optional Sync

- 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

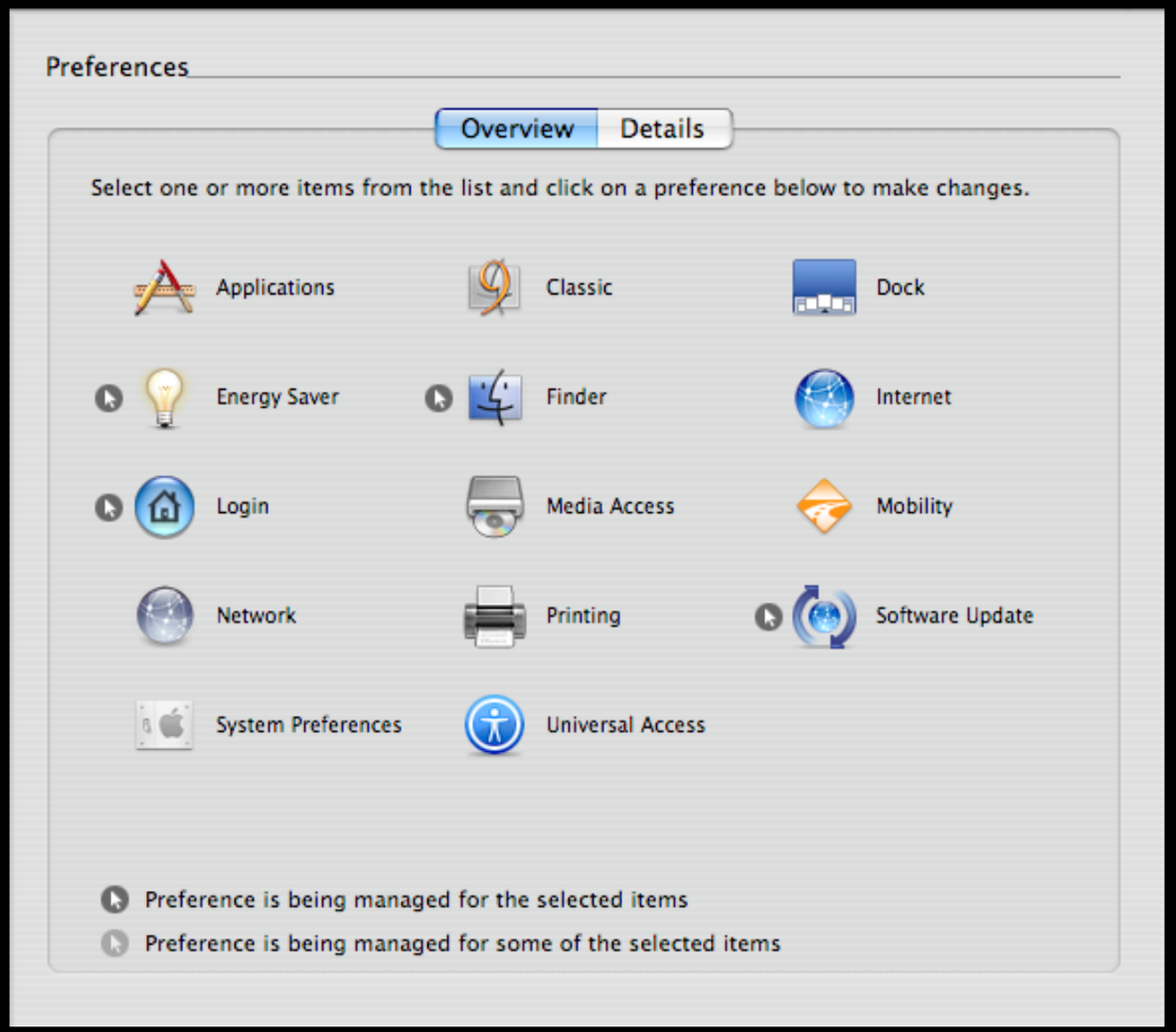


Mobile Accounts and Management

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

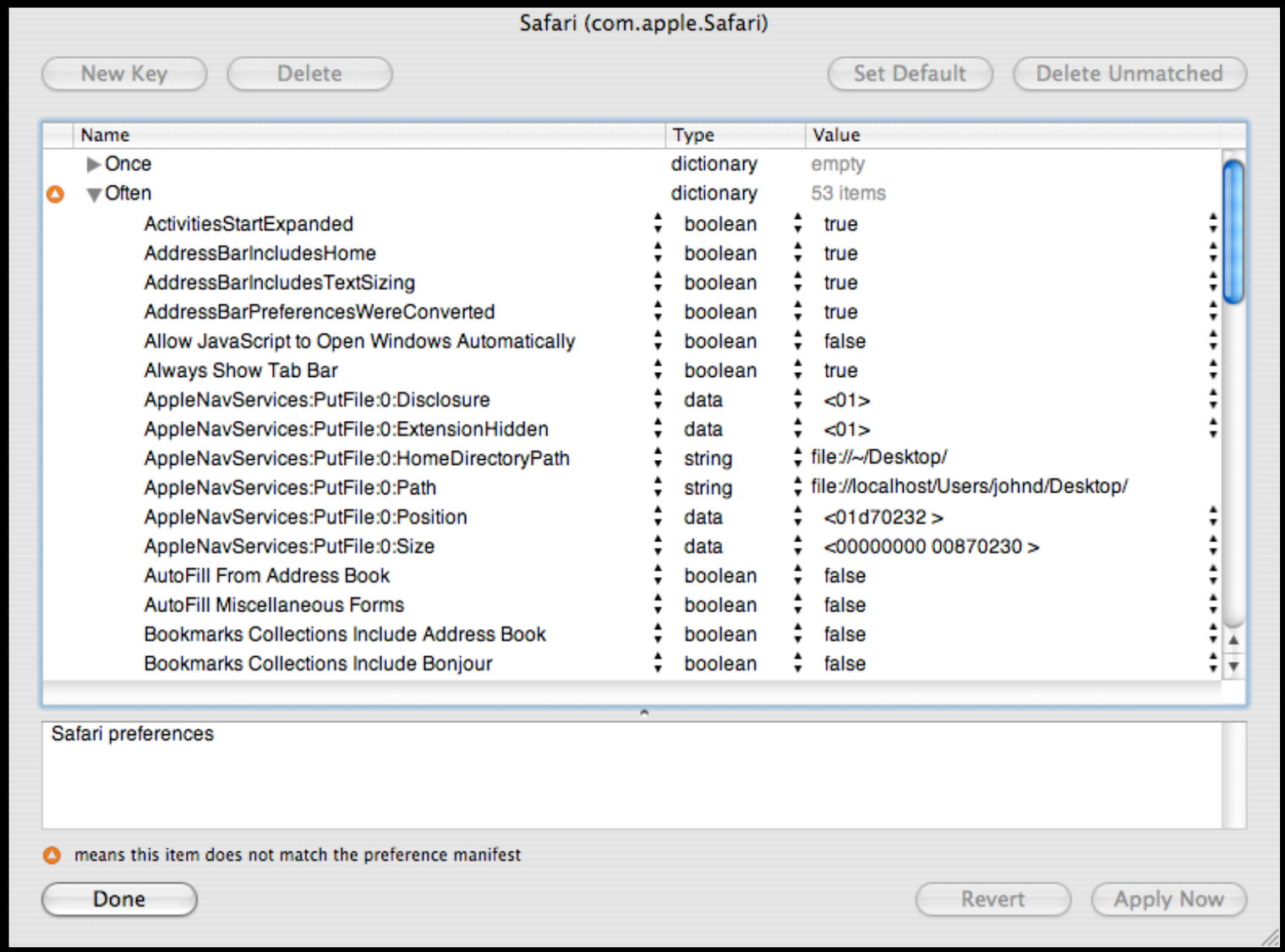
Attention to Detail(s)

Managing non-System Preferences



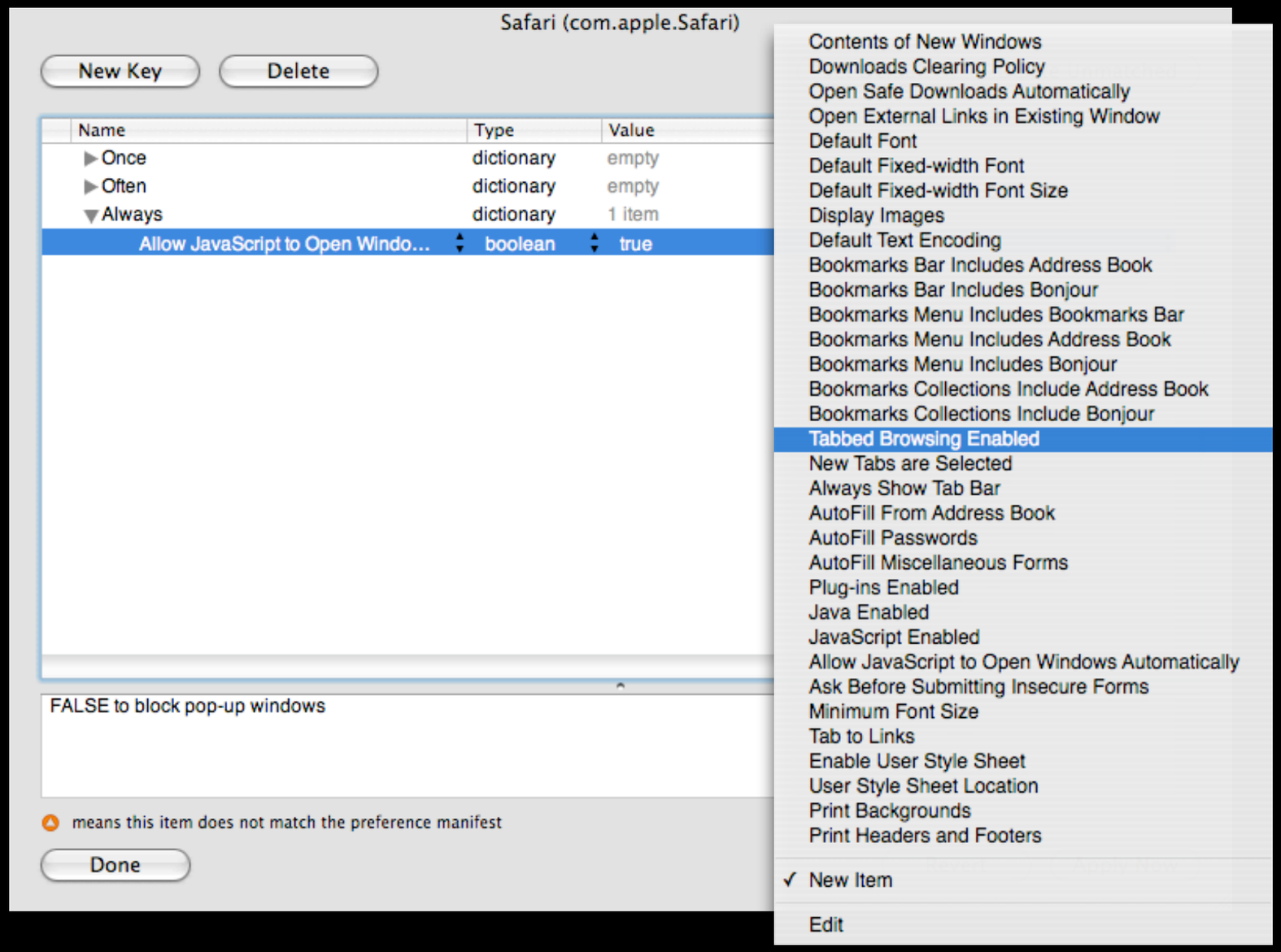
Preference Editor

Granular control



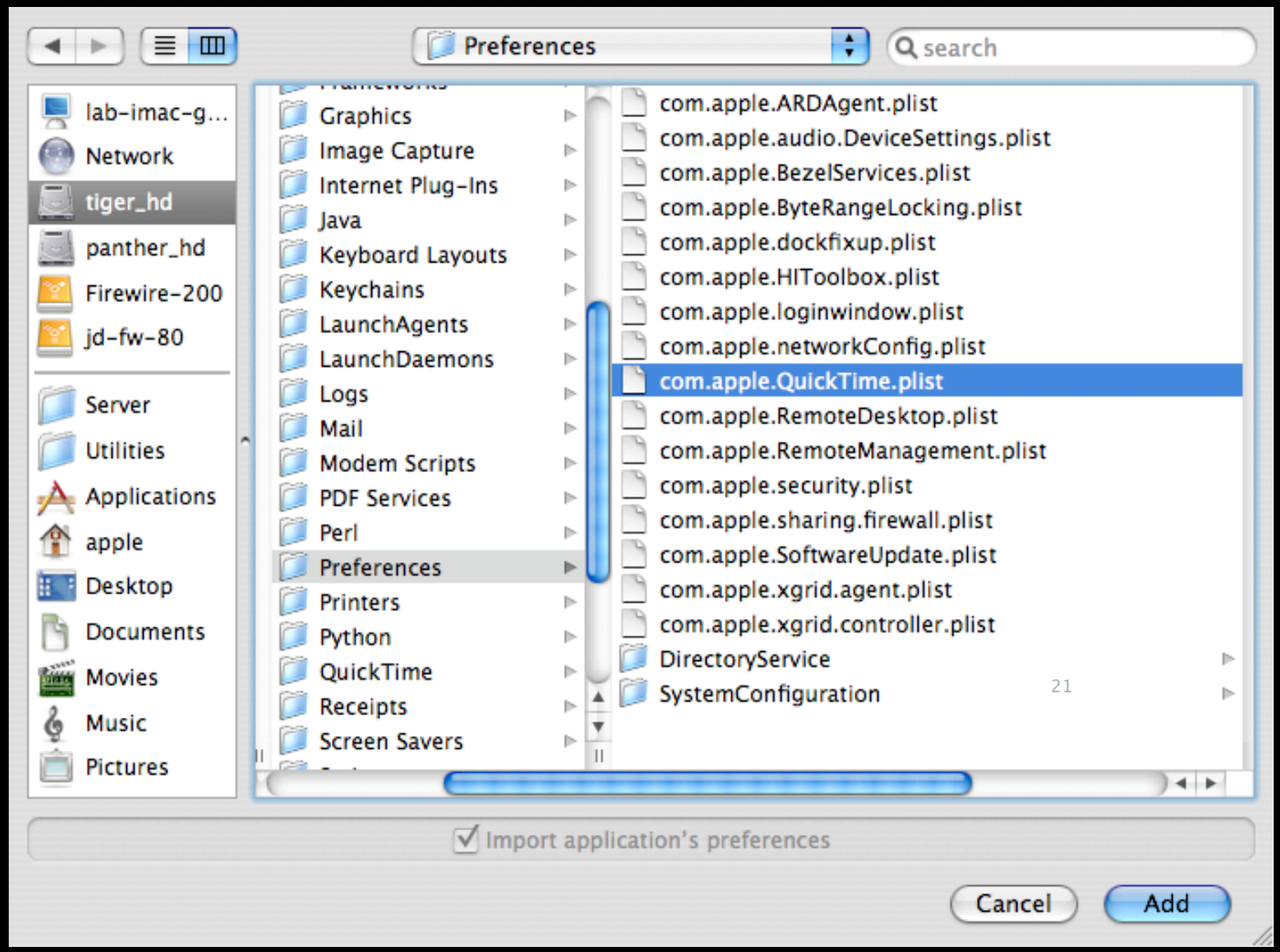
Preference Manifest

Built-in management



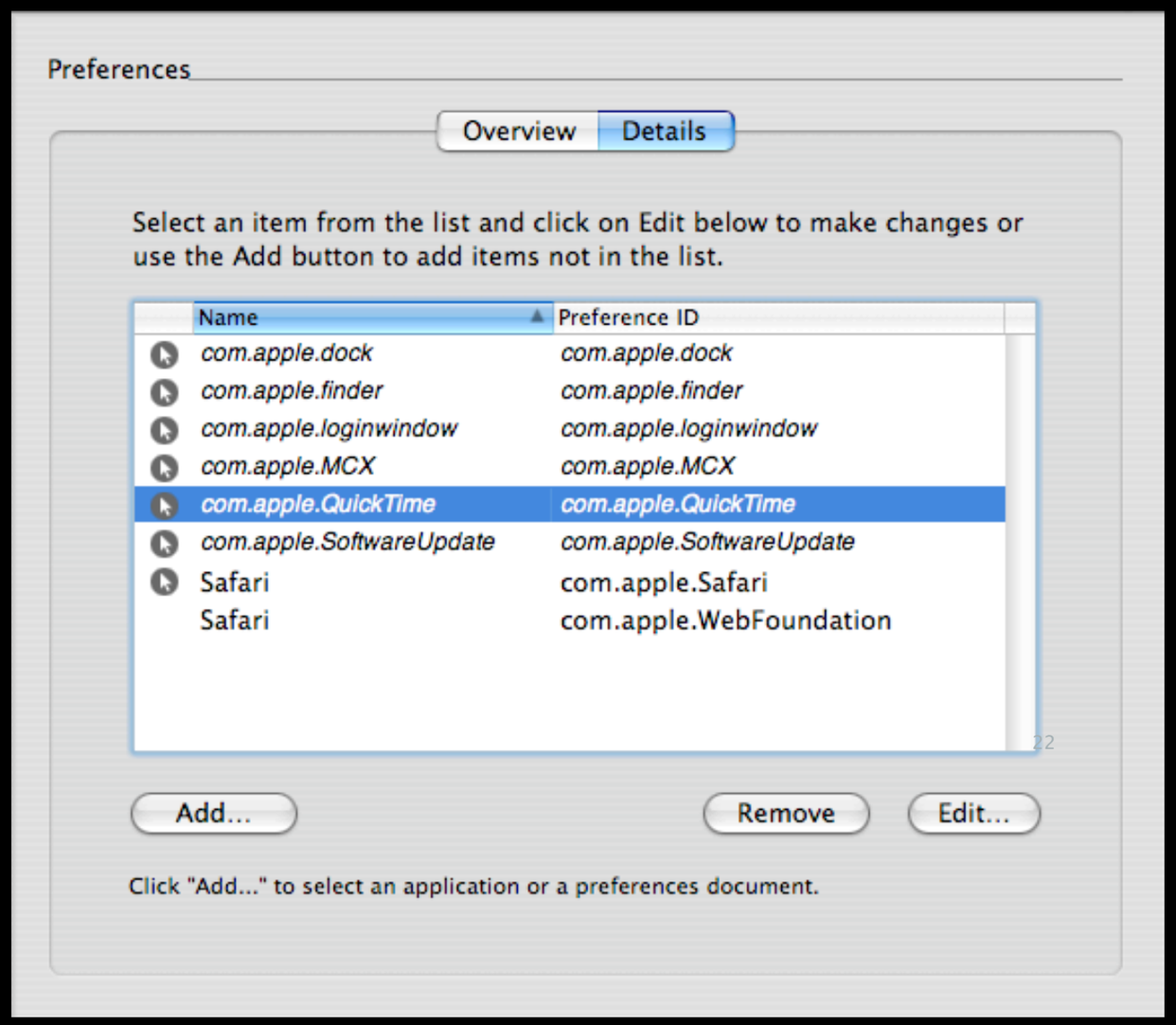
Adding normal preferences

Using admin defined preferences



QTPro—For Everyone

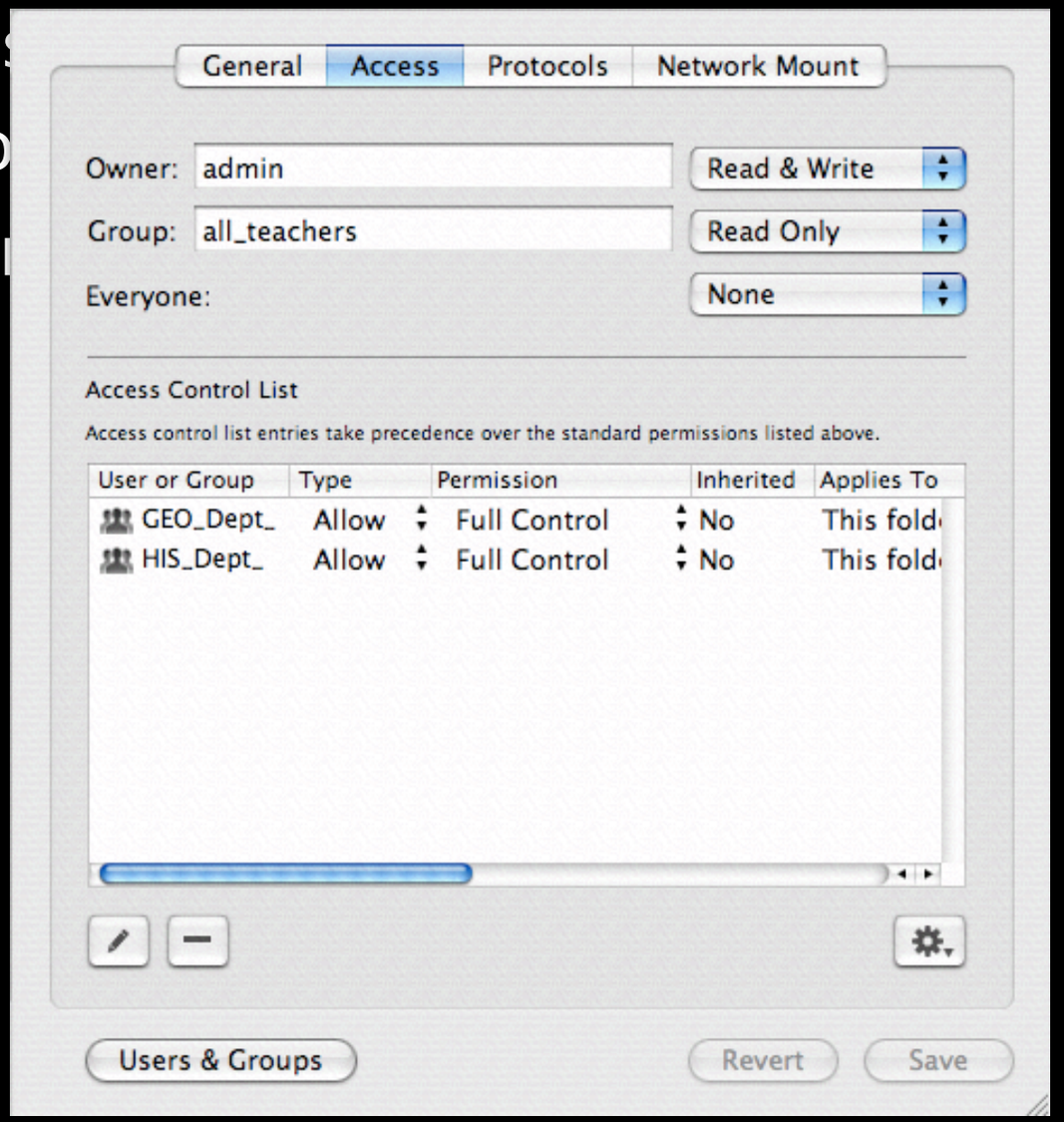
All QT prefs applied—incl. serial number



Access Control Lists (ACLs)

A kazillion ways to configure access to files / folders

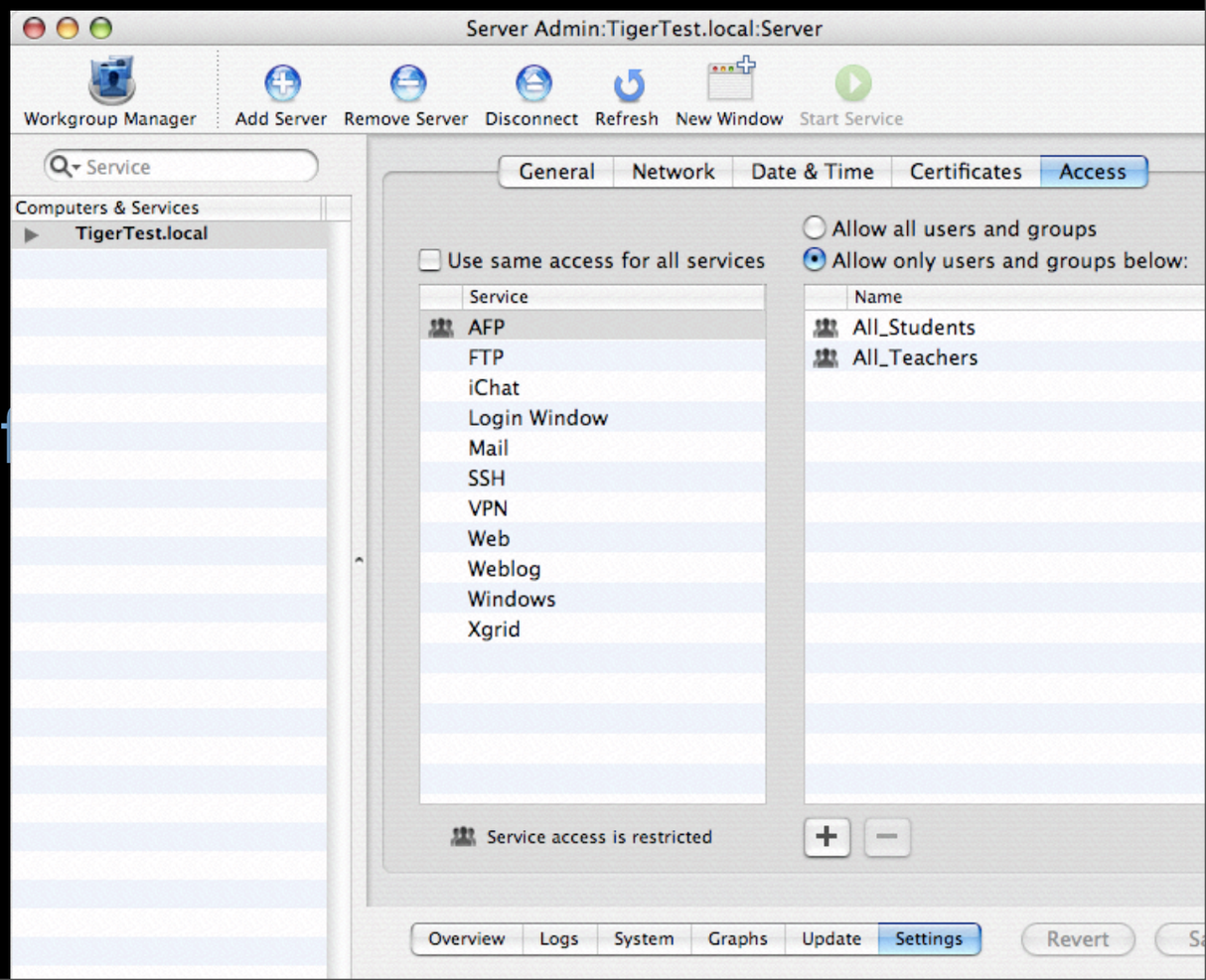
- Provides an extended set of permissions for a file or folder
- Allows you to set permissions for multiple users and groups
  - simulates them being owners or groups
- Groups can be nested within other gro
- Contain a series of Access Control Entr
  - an ordered list of permissions
- Work in addition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