Managing Tigers

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

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



	Accounts Available	
Play nice	anaged Lab Client e and be good to Tenshi neans give her treats)	
	Apple Barber Scott Bevins Jayson	
	Brenner Sandy	A V
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 conrol Software Update

	Overview Details]
elect one or more items from	the list and click on a prefe	rence below to make changes.
Applications	Q Classic	Dock
Energy Saver	O 🗳 Finder	Internet
🕽 🙆 Login	Media Access	Mobility
Network	Printing	🗴 🧑 Software Update
System Preferences	Universal Access	
	3	
Preference is being mana	ged for the selected items	
Preference is being mana	ged for some of the selected	l items

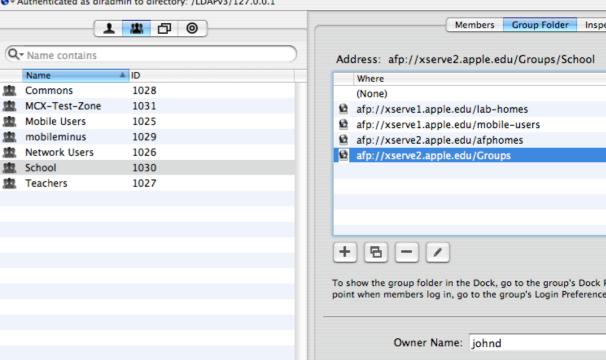
Management is more than user passwords

- 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 modified Authenticated as diradmin to directory: /LDAPv3/127.0.0.1
- 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

000	Workgroup Mana	ager: xserve2.apple.edu	
Admin Sharing Network	Accounts Preferences New User Delete Connect	Disconnect Refresh New Window Search	
	Share Points All	General Access Protocols	Network Mount
📁 Mr Couch	📁 Hand In	- <u> </u>	
📁 Mr DeTroye 🛛 🕨	📁 Projects 🔹 🕨	Owner: jcouch	Read & Write
	🃁 Take One 🛛 🖻	Group: math	Write Only
		Everyone:	None
		Access Control List Access control list entries take precedence over the standard	permissions listed above.
		User or Group Type Permission	Inherited Applies To
		Couch John Allow + Full Control	No This fold:

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

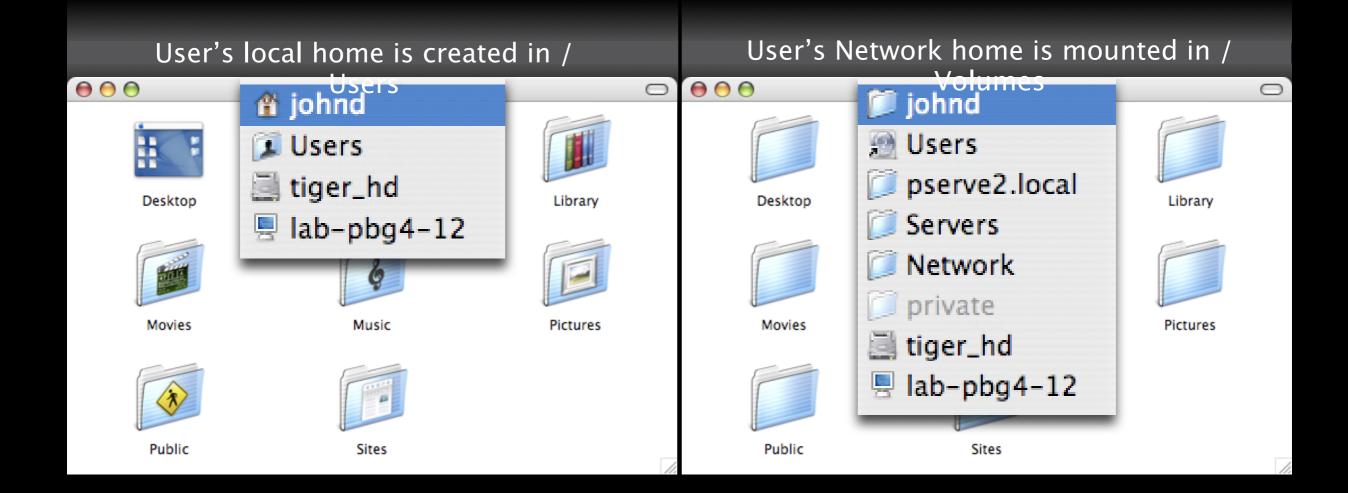
Basic Advanced Groups H	Home Mail	Print Quota Info Windows Inspector	original_node_name	/LDAPv3/pserve1.apple.edu
Filter:	Reco	ord Size: 4.70 KB	▶ name	(johnd, DeTroye John)
			mcx_flags	xml version="1.0" encoding="UTF</td
Name	Size	Value	home	/Users/johnd
AppleMetaNodeLocation	17 bytes	/LDAPv3/127.0.0.1	original_authentication_authority	(;ApplePasswordServer;0x427ed4200.
AuthenticationAuthority(2)	837 bytes	;ApplePasswordServer;	authentication_authority	;LocalCachedUser;/LDAPv3/pserve1
GeneratedUID	36 bytes	F82066D6-E152-4C3F-91A2-		,LOCAICACHEGOSEI,/LDAPVS/pserve1
HomeDirectory	79 bytes	<home_dir><url>afp://</url></home_dir>	passwd	
Keywords	7 bytes	primary	lastname	99
LastName	2 bytes	99	_writers_picture	johnd
MCXFlags	283 bytes	xml version="1.0" encoding="UTF-</td <td>realname</td> <td>DeTroye John</td>	realname	DeTroye John
MCXSettings(2)	3.29 KB	xml version="1.0" encoding="UTF-</td <td>uid</td> <td>10125</td>	uid	10125
NFSHomeDirectory	42 bytes	/Network/Servers/pserve2.local/User		
Password	8 bytes	******	original_home	/Network/Servers/pserve2.local/User
Picture	28 bytes	/Library/UserPics/johnd.tiff	preserved_attributes	(dsAttrTypeStandard:AuthenticationA
PrimaryGroupID	2 bytes	20	shell	/bin/bash
RealName	12 bytes	DeTroye John	generateduid	F82066D6-E152-4C3F-91A2-B018E.
► RecordName(2)	17 bytes	johnd	gid	20
RecordType	23 bytes	dsRecTypeStandard:Users	mcx_settings	(xml version="1.0" encoding="UTF</td
) 4 ►	original_home_loc	<home_dir><url>afp://pserve2.appl</url></home_dir>
Options (Edit) ((New Value) (New Attribute)) copy_timestamp	2005-05-22T20:43:41Z
			picture	/Library/UserPics/johnd.tiff

Network Directory (OpenLDAP)

Local Directory (NetInfo)



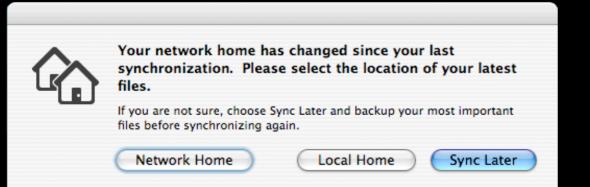
Mobile Account Home Directories Local and Network home directories



Portable Home Directories

Tiger feature – <u>not</u> 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

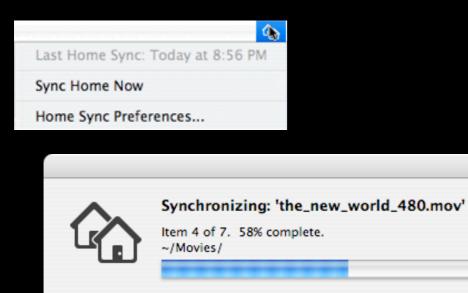


	Synchronization	n Rules			
Login & Log	jout Sync Back	ground Sync	Options		
Manage: (Never	Once	Always		
Settings apply	to mobile accounts	on Mac OS X v10.4	4 and later.		
Synchronize at login a	and logout:				
Folder			- +		
~/Desktop					
~/Documents			-		
~/Homework			¥ ¯		
~/Library			•		
Chin items that match					
Skip items that match	any of the follow	/ing:			
	Path				
Full Path Full Path					
Full Path					
Full Path	Logi	n a Logoat Sync	background sync	options	
runradi	Manage:	🔘 Never	Once	Always	
Merge with user	Settin	as apply to mobile	accounts on Mac OS X v10.	4 and later.	
				- and later.	
	Conselsors along the loss	the background	1:		
	· · · · · · · · · · · · · · · · · · ·	the background			
	Folder	and background		(
		and background			
	Folder				
	Folder				
	Folder				
	Folder ~				
	Folder ~	t match any of th	he following:		
	Folder ~ Skip items that	t match any of th String, file, c	he following:		
	Folder ~ Skip items that Match	t match any of th String, file, c ‡ ~/Library	he following:		
	Folder ~ Skip items that Match Full Path	t match any of th String, file, c ‡ ~/Library ‡ ~/.Trash	he following:	Entourage	
	Folder ~ Skip items that Match Full Path Full Path	t match any of th String, file, c † ~/Library † ~/.Trash † ~/Documen	he following: or folder	-	
	Folder ~ Skip items that Match Full Path Full Path Full Path	t match any of th String, file, c † ~/Library † ~/.Trash † ~/Documen	he following: or folder nts/Microsoft User Data/	-	

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

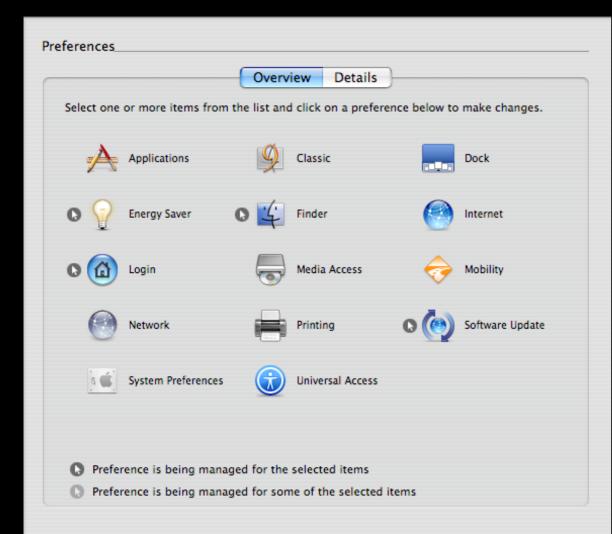
	Synchronization Rules					
Lo	gin & Logout Sync	Background Sync	Options			
Manage:	ONever	Once	Always			
	background folders	ccounts on Mac OS X v10				
,						

Stop

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

	Overview Deta		
elect one or more items from th	te list and click on a pr	eference below to make char	iges.
Applications	Gassic	Dock	
🔉 💡 Energy Saver 🛛	Finder	Internet	
🕽 🙆 Login	Media Access	Mobility	
Network	Printing	🖸 🧑 Software U	pdate
System Preferences	Universal Acc	ess	
Preference is being manage Preference is being manage			

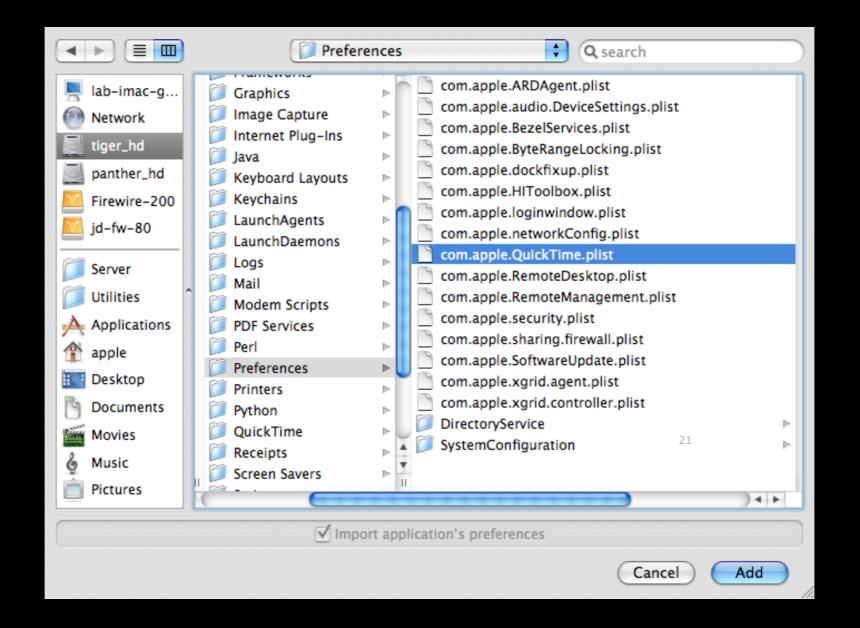
Preference Editor Granular control

 ▶Once Ø Often ActivitiesStartExpanded ActivitiesStartExpanded AddressBarlncludesHome AddressBarlncludesTextSizing boolean true AddressBarlncludesTextSizing boolean true AddressBarPreferencesWereConverted boolean true Allow JavaScript to Open Windows Automatically boolean true Allow JavaScript to Open Windows Automatically boolean true Always Show Tab Bar AppleNavServices:PutFile:0:Disclosure data <01> AppleNavServices:PutFile:0:HomeDirectoryPath AppleNavServices:PutFile:0:Path tring file://ocalhost/Users/johnd/Desktop/ AppleNavServices:PutFile:0:Size data <01070232 > AppleNavServices:PutFile:0:Size data <00000000 00870230 > AutoFill From Address Book boolean false 		Name		Туре	Value	
ActivitiesStartExpandedbooleantrueAddressBarlncludesHomebooleantrueAddressBarlncludesTextSizingbooleantrueAddressBarPreferencesWereConvertedbooleantrueAllow JavaScript to Open Windows AutomaticallybooleanfalseAlways Show Tab BarbooleantrueAppleNavServices:PutFile:0:Disclosuredata<01>AppleNavServices:PutFile:0:ExtensionHiddendata<01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata<01d70232 >AppleNavServices:PutFile:0:Sizedata<000000000870230 >AutoFill From Address BookbooleanfalseAutoFill Miscellaneous FormsbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		▶ Once		dictionary	empty	
AddressBarlncludesHome+boolean+trueAddressBarlncludesTextSizing+boolean+trueAddressBarPreferencesWereConverted+boolean+trueAllow JavaScript to Open Windows Automatically+boolean+trueAllow JavaScript to Open Windows Automatically+boolean+trueAlways Show Tab Bar+boolean+trueAppleNavServices:PutFile:0:Disclosure+data+<01>AppleNavServices:PutFile:0:ExtensionHidden+data+<<01>AppleNavServices:PutFile:0:HomeDirectoryPath+string+file://~/Desktop/AppleNavServices:PutFile:0:Position+data+<<01d70232 >AppleNavServices:PutFile:0:Size+data+<<00000000 00870230 >AutoFill From Address Book+boolean+falseBookmarks Collections Include Address Book+boolean+false	2	▼ Often		dictionary	53 items	
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:HomeDirectoryPath + string + file://~/Desktop/ AppleNavServices:PutFile:0:Path + string + file://localhost/Users/johnd/Desktop/ AppleNavServices:PutFile:0:Position + data + <01070232 > 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		ActivitiesStartExpanded	ŧ	boolean	true	\$
AddressBarPreferencesWereConvertedbooleantrueAllow JavaScript to Open Windows AutomaticallybooleanfalseAlways Show Tab BarbooleanfalseAppleNavServices:PutFile:0:Disclosuredata<01>AppleNavServices:PutFile:0:ExtensionHiddendata<01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://~/Desktop/AppleNavServices:PutFile:0:Pathstringfile://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata<01d70232 >AppleNavServices:PutFile:0:Sizedata<00000000 00870230 >AutoFill From Address BookbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		AddressBarIncludesHome	ŧ	boolean	true true	\$
Allow JavaScript to Open Windows AutomaticallybooleanfalseAlways Show Tab BarbooleantrueAppleNavServices:PutFile:0:Disclosuredata<01>AppleNavServices:PutFile:0:ExtensionHiddendata<01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://~/Desktop/AppleNavServices:PutFile:0:Pathstringfile://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata<01d70232 >AppleNavServices:PutFile:0:Sizedata<0000000000870230 >AutoFill From Address BookbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		AddressBarIncludesTextSizing	ŧ	boolean	true	÷
Always Show Tab BarbooleantrueAppleNavServices:PutFile:0:Disclosuredata<01>AppleNavServices:PutFile:0:ExtensionHiddendata<01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://~/Desktop/AppleNavServices:PutFile:0:Pathstringfile://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata<01d70232 >AppleNavServices:PutFile:0:Sizedata<0000000000870230 >AutoFill From Address BookbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		AddressBarPreferencesWereConverted	ŧ	boolean	true	÷ 🗂
AppleNavServices:PutFile:0:Disclosuredata<01>AppleNavServices:PutFile:0:ExtensionHiddendata<01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://~/Desktop/AppleNavServices:PutFile:0:Pathstringfile://localhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata<01170232 >AppleNavServices:PutFile:0:Sizedata<000000000870230 >AppleNavServices:PutFile:0:SizebooleanfalseAutoFill From Address BookbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		Allow JavaScript to Open Windows Automatically	ŧ	boolean	false	÷
AppleNavServices:PutFile:0:ExtensionHiddendata< <01>AppleNavServices:PutFile:0:HomeDirectoryPathstringfile://~/Desktop/AppleNavServices:PutFile:0:Pathstringfile://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Positiondata< <01d70232 >AppleNavServices:PutFile:0:Sizedata< <0000000 00870230 >AutoFill From Address BookbooleanfalseAutoFill Miscellaneous FormsbooleanfalseBookmarks Collections Include Address Bookbooleanfalse		Always Show Tab Bar	ŧ	boolean	true true	÷
AppleNavServices:PutFile:0:HomeDirectoryPath* string* file://~/Desktop/AppleNavServices:PutFile:0:Path* string* file://ocalhost/Users/johnd/Desktop/AppleNavServices:PutFile:0:Position* data* <01d70232 >AppleNavServices:PutFile:0:Size* data* <000000000870230 >AutoFill From Address Book* boolean* falseAutoFill Miscellaneous Forms* boolean* falseBookmarks Collections Include Address Book* boolean* false		AppleNavServices:PutFile:0:Disclosure	ŧ	data	↓ <01>	÷
AppleNavServices:PutFile:0:Path string file://localhost/Users/johnd/Desktop/ AppleNavServices:PutFile:0:Position 		AppleNavServices:PutFile:0:ExtensionHidden	ŧ	data	↓ <01>	÷
AppleNavServices:PutFile:0:Position+data+<01d70232 >AppleNavServices:PutFile:0:Size+data+<0000000 00870230 >AutoFill From Address Book+boolean+falseAutoFill Miscellaneous Forms+boolean+falseBookmarks Collections Include Address Book+boolean+false		AppleNavServices:PutFile:0:HomeDirectoryPath	ŧ	string	file://~/Desktop/	
AppleNavServices:PutFile:0:Size data data dolean data dolean data dolean data dolean false boolean false boolean false		AppleNavServices:PutFile:0:Path	ŧ	string	file://localhost/Users/johnd/Desktop/	
AutoFill From Address Book\$ boolean\$ falseAutoFill Miscellaneous Forms\$ boolean\$ falseBookmarks Collections Include Address Book\$ boolean\$ false		AppleNavServices:PutFile:0:Position	ŧ	data	<pre><01d70232 ></pre>	÷
AutoFill Miscellaneous Forms Bookmarks Collections Include Address Book boolean boolean boolean false boolean false		AppleNavServices:PutFile:0:Size	ŧ	data	<0000000 00870230 >	÷
Bookmarks Collections Include Address Book 🕴 boolean 💠 false		AutoFill From Address Book	ŧ	boolean	false	÷
		AutoFill Miscellaneous Forms	ŧ	boolean	false	\$
Bookmarks Collections Include Boniour		Bookmarks Collections Include Address Book	ŧ	boolean	false	+ -
		Bookmarks Collections Include Bonjour	ŧ	boolean	false	÷.
Safari preferences		fari proforonoco	^			_

Preference Manifest Built-in management

	Safari (c	om.apple.Safari)	Contents of New Windows
			Downloads Clearing Policy
New Key Delete			Open Safe Downloads Automatically
			Open External Links in Existing Window
Name	Туре	Value	Default Font
▶ Once	dictionary	empty	Default Fixed-width Font
▶Often	dictionary	empty	Default Fixed-width Font Size
▼Always	dictionary	1 item	Display Images
Allow JavaScript to Open Windo	boolean	true	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
FALSE to block pop-up windows		<u> </u>	Ask Before Submitting Insecure Forms Minimum Font Size
			Tab to Links
			Enable User Style Sheet
			User Style Sheet Location
			Print Backgrounds
O means this item does not match the preference	ce manifest		Print Headers and Footers
Done			
Done			✓ New Item
			Edit

Adding normal preferences Using admin defined preferences



QTPro—For Everyone All QT prefs applied—incl. serial number

	ct an item from the list and the Add button to add items	click on Edit below to make change	s or
use			
		Preference ID	
0	com.apple.dock	com.apple.dock	
0	com.apple.finder	com.apple.finder	
0	com.apple.loginwindow	com.apple.loginwindow	
0	com.apple.MCX	com.apple.MCX	
	com.apple.QuickTime	com.apple.QuickTime	
0	com.apple.SoftwareUpdate	com.apple.SoftwareUpdate	
0	Safari	com.apple.Safari	
	Safari	com.apple.WebFoundation	
			22
	Add	(Remove) (Edi	.)
-	4dd	Kemove Edi)

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 group
- Groups can be nested within other gro
- Contain a series of Access Control Entre an ordered list of permissions
- Work in addition to the standard POSIX permissions

up Type ept_ Allow	edence over the standard Permission Full Control Full Control	Read & Read Or None permissions listed Inherited No No	nly ‡
ol List ist entries take preco up Type ept_ Allow	Permission Full Control	None permissions listed Inherited No	d above. Applies To This fold
ist entries take preci up Type ept_ Allow	Permission Full Control	permissions listed Inherited \$ No	d above. Applies To This fold
ist entries take preci up Type ept_ Allow	Permission Full Control	Inherited \$ No	Applies To This fold
up Type ept_ Allow	Permission Full Control	Inherited \$ No	Applies To This fold
		¥ NO	
			÷.

Service Access Control Lists (SACLs)

• VPN

• Web

• Weblog

Xgrid

• Windows

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

- •AFP
- FTP
- iChat
- •Login Window
- Mail
- •SSH

Another layer of control on top of POSIX and ACLs

$\Theta \Theta \Theta$		Server Admin:TigerTest.local:Set	erver
Workgroup Manager	Add Server R	emove Server Disconnect Refresh New Window	v Start Service
Q- Service			ate & Time Certificates Access
Computers & Services TigerTest.local		Use same access for all services	 Allow all users and groups Allow only users and groups below:
		Service AFP FTP iChat Login Window Mail SSH VPN Web Weblog Windows Xgrid	Name All_Students All_Teachers
		Service access is restricted	+ - Update Settings Revert Sa