Mac OS X Accounts

Session M235

Macworld San Francisco 2005

John Stewart & Dave Pugh

University of Michigan

Apple Certified System Administrators 10.3

Apple Certifications for 10.3.x

Course Names	Certification Level	Length (days)
Mac OS X Help Desk Essentials	ACHDS	3
Mac OS X Server Essentials	ACTC (with Help Desk Essentials)	4
System Administration of Mac OS X Clients	Apple Certified System Administrator	5 days each course
System Administration using Mac OS X Server		

train.apple.com • 800-848-6398

You think it’s all about the username and password. Think again.

What We'll Cover

- What are accounts, where they live, and their care and feeding
- When to use NetInfo Manager
- Going to town with Workgroup Manager
- Some command line goodies

Why You Need To Know This

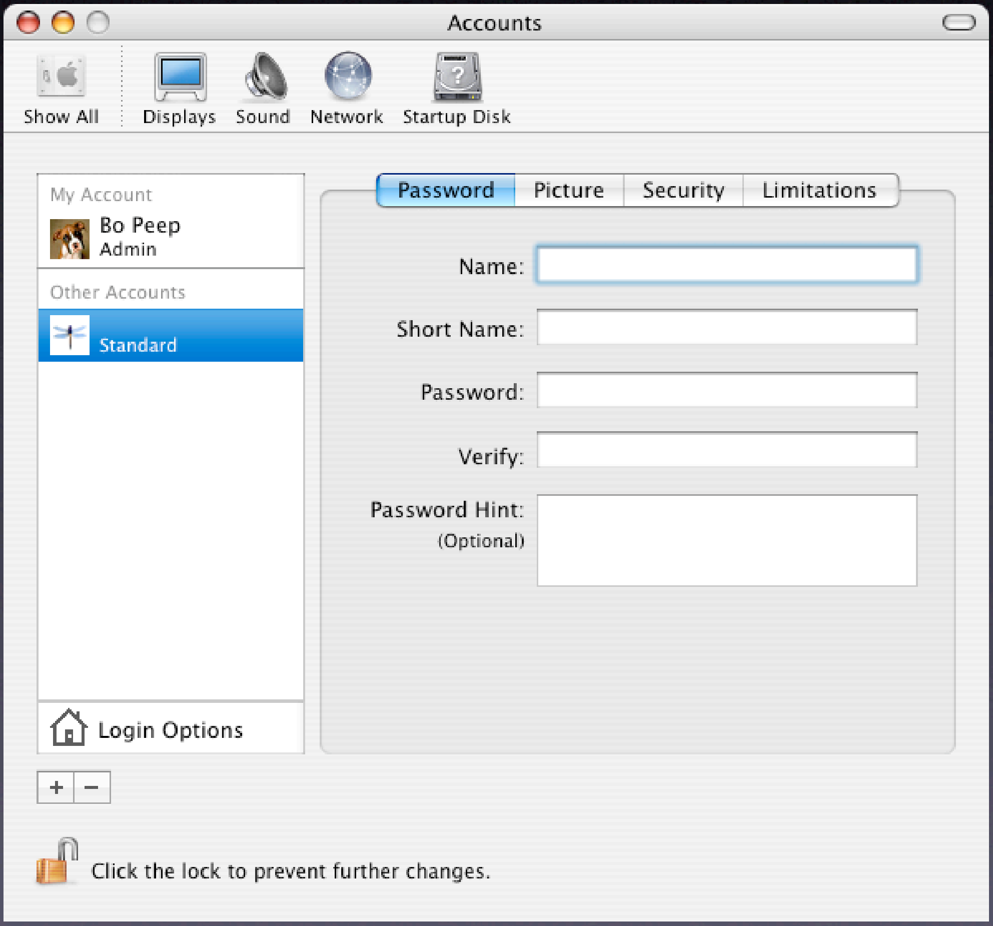
- With this information, you can provide management over a single Mac, or a deployment of many Macs with a deeper level of control

Where this is useful

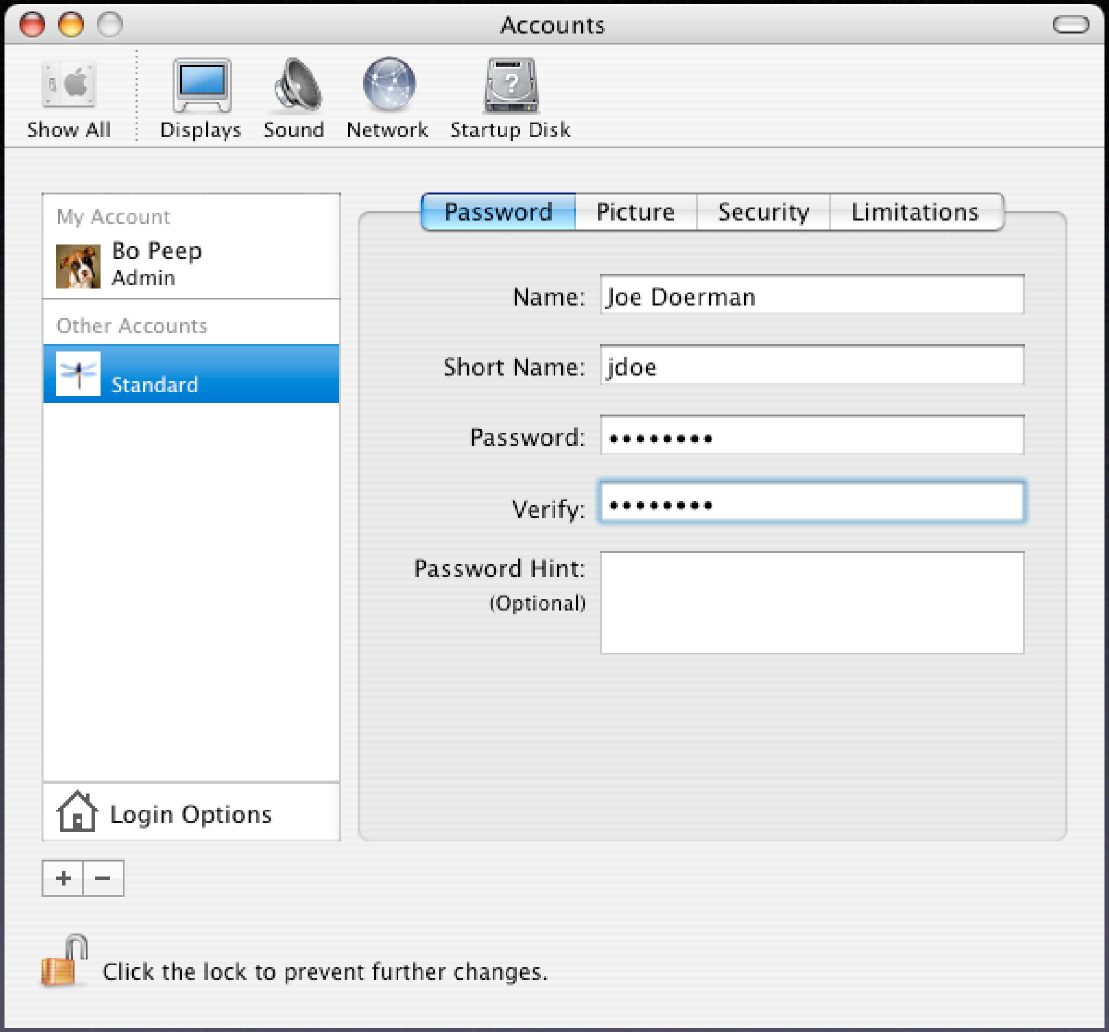
- Managing non-networked machines (notebooks)
- Small-scale lab or workplace deployments that don’t have OS X Server
- Macs at home

Accounts

Creating an Account the “Normal” way



Click the lock to prevent further changes.



Name: Joe Doerman

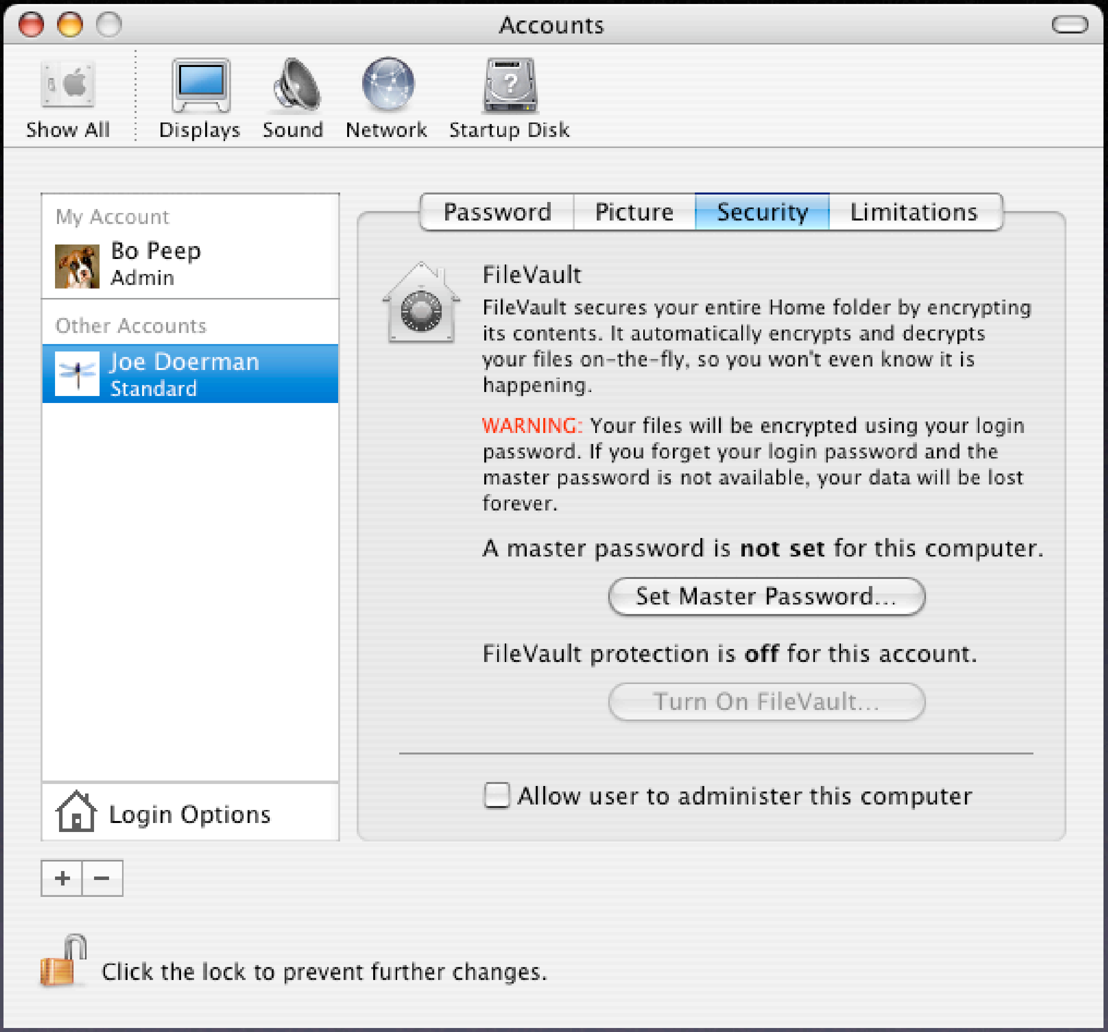
Short Name: jdoe

Password: ••••••••

Verify: ••••••••

Password Hint: (Optional)

Click the lock to prevent further changes.



FileVault

FileVault secures your entire Home folder by encrypting its contents. It automatically encrypts and decrypts your files on-the-fly, so you won't even know it is happening.

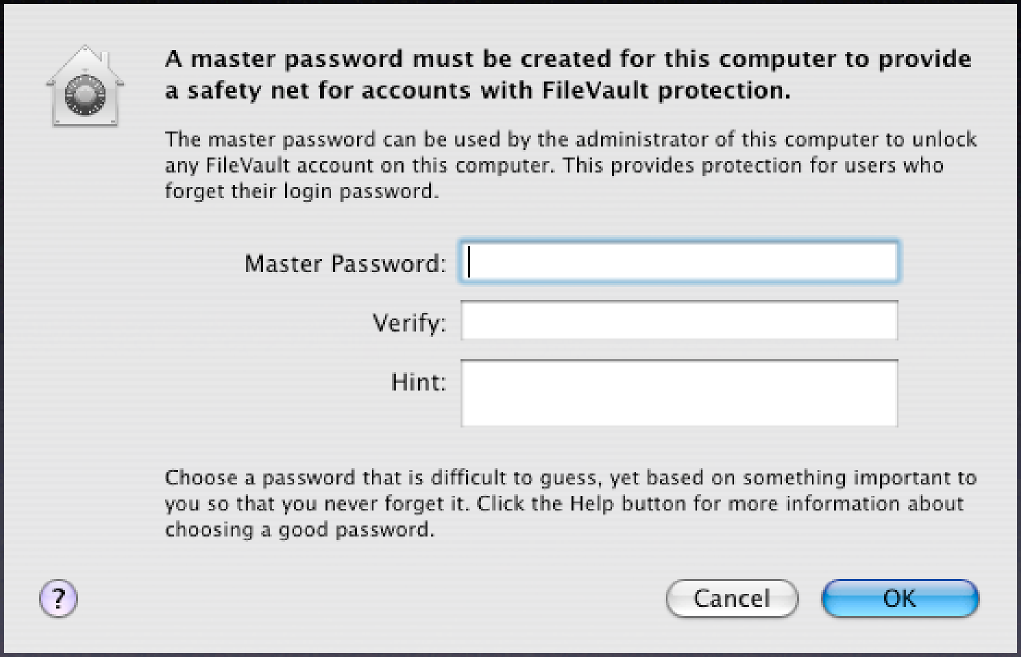
WARNING: Your files will be encrypted using your login password. If you forget your login password and the master password is not available, your data will be lost forever.

A master password is **not set** for this computer.

FileVault protection is **off** for this account.

☐ Allow user to administer this computer

Click the lock to prevent further changes.



A master password must be created for this computer to provide a safety net for accounts with FileVault protection.

The master password can be used by the administrator of this computer to unlock any FileVault account on this computer. This provides protection for users who forget their login password.

Master Password:

Verify:

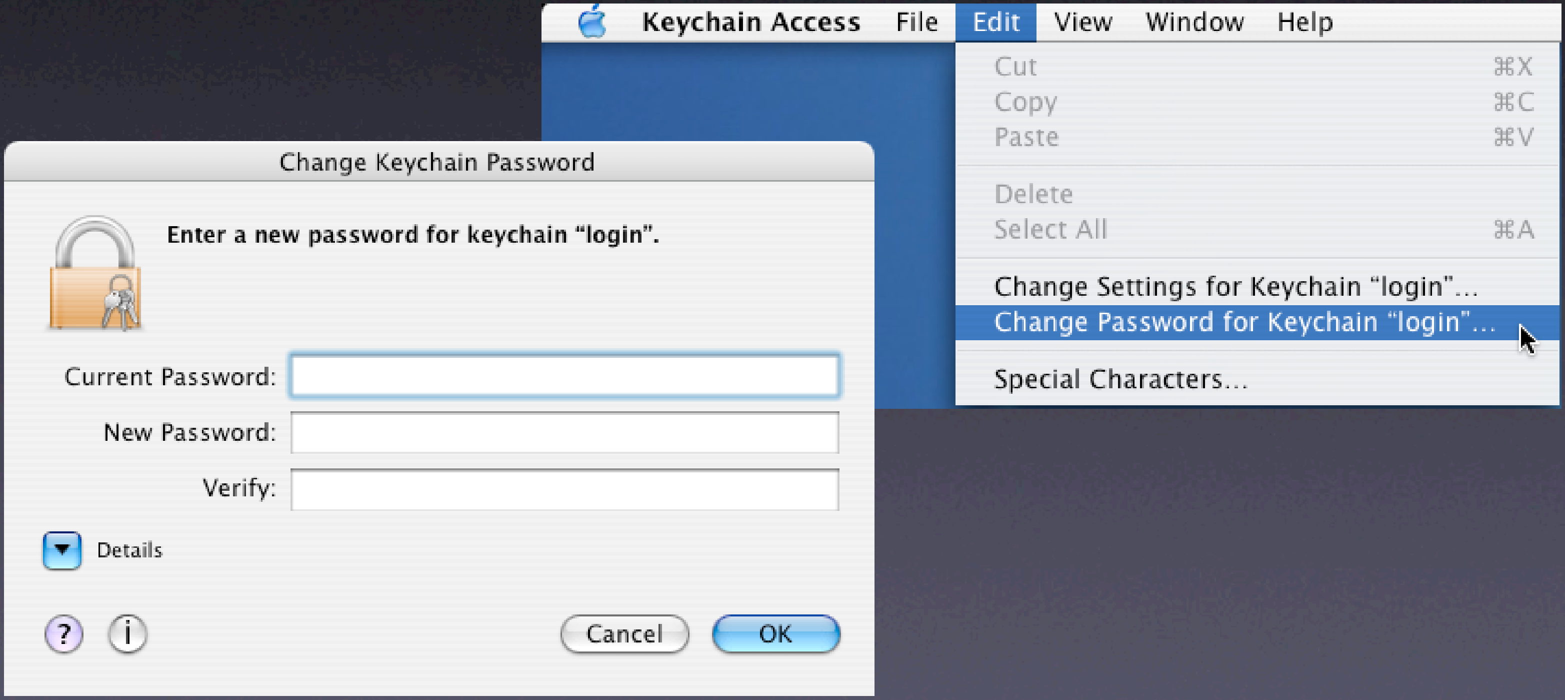
Hint:

Choose a password that is difficult to guess, yet based on something important to you so that you never forget it. Click the Help button for more information about choosing a good password.

Should I set the Master Password?

Reasons for	Reasons against
Setting the Master Password enables you to reset a forgotten password.	You can still recover a lost password using the install disk.
NOT setting the Master Password will allow another admin user to set it.	There is no recovering a lost master password. You must reformat the disk to set a new master password.

How do I set a “safe” password (and how do I check it)?



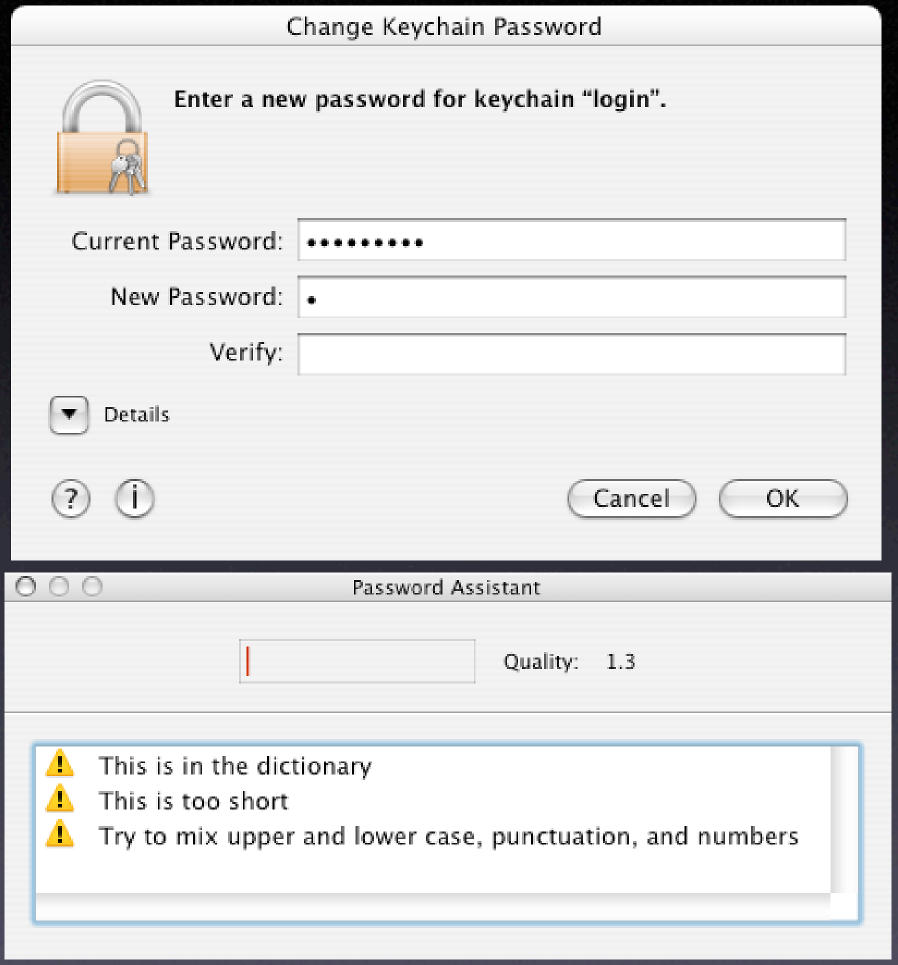
Change Keychain Password

Enter a new password for keychain “login”.

Current Password:

New Password:

Verify:



Change Keychain Password

Enter a new password for keychain “login”.

Current Password: ••••••••••

New Password: •

Verify:

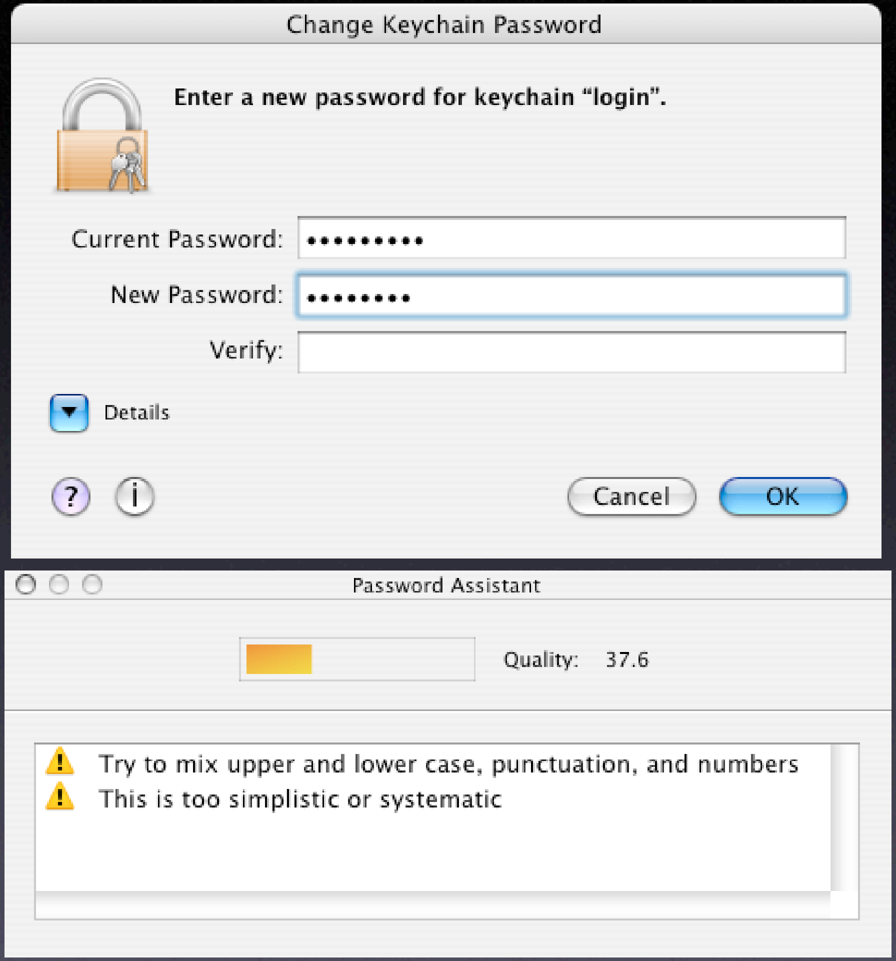
Password Assistant

Quality: 1.3

⚠ This is in the dictionary

⚠ This is too short

⚠ Try to mix upper and lower case, punctuation, and numbers



Enter a new password for keychain “login”.

Current Password: ••••••••••

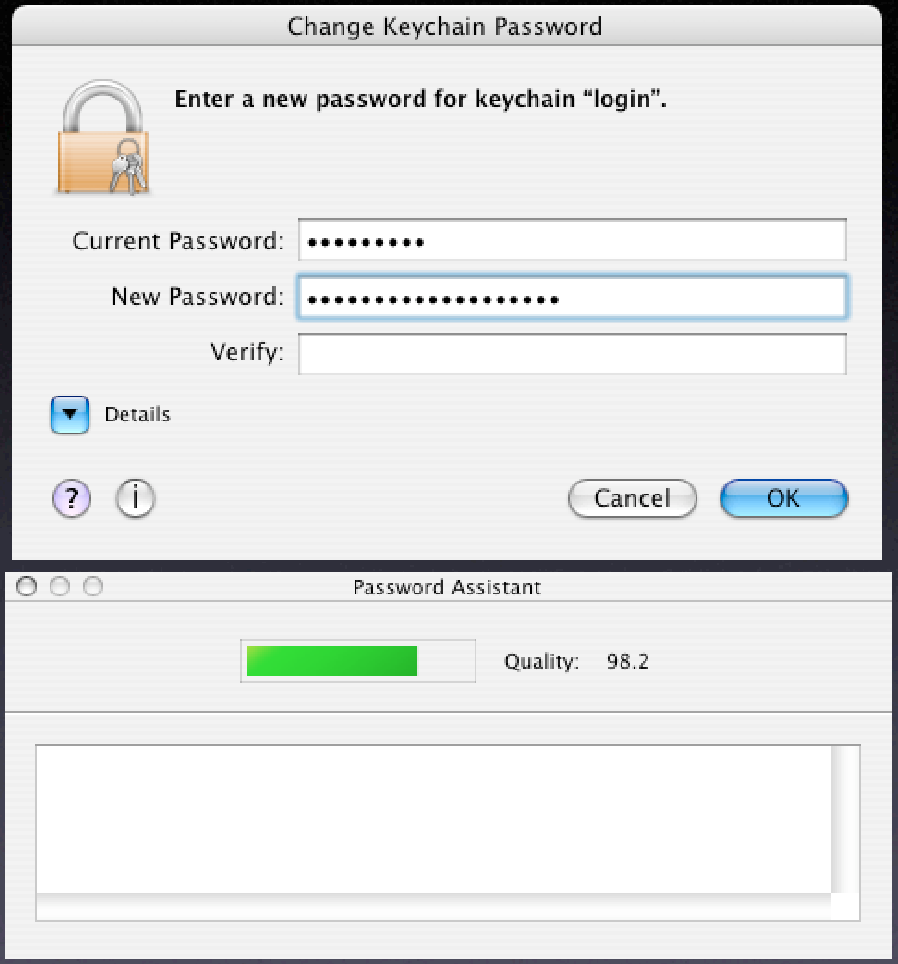
New Password: •••••••••

Verify:

Quality: 37.6

⚠ Try to mix upper and lower case, punctuation, and numbers

⚠ This is too simplistic or systematic



Change Keychain Password

Enter a new password for keychain “login”.

Current Password: •••••••••

New Password: •••••••••••••••••••

Verify:

Password Assistant

Quality: 98.2

Where are passwords stored?

- The password hash is stored in a shadow file at /var/db/shadow/hash/*generateduid*
- Crypt passwords are no more (since 10.3.0)

In case you're wondering what a "generated uid" is...

A guaranteed-to-be-unique identifier that appears in a user's NetInfo database record

- e.g.: 68753A44-4D6F-1226-9C60-0050E4C00067
- for more, read the `uuidgen` manpage

Creating an Account from the Command Line

(For the Deliberate Contortionist)

```
sudo nicl . -create /users/jdoe uid 12000
sudo nicl . -create /users/jdoe gid 20
sudo nicl . -create /users/jdoe shell /bin/tcsh
sudo nicl . -create /users/jdoe home /Users/jdoe
sudo nicl . -create /users/jdoe realname “Jason Doerman”
sudo nicl . -create /users/jdoe passwd “*”
sudo nicl . -create /users/jdoe picture “/Library/User Pictures/Animals/Jaguar.tif”
sudo nicl . -create /users/jdoe hint “”
sudo nicl . -create /users/jdoe sharedDir Public
sudo nicl . -create /users/jdoe _writers_passwd jdoe
sudo nicl . -create /users/jdoe _writers_tim_passwd jdoe
sudo nicl . -create /users/jdoe _writers_hint jdoe
sudo nicl . -create /users/jdoe _writers_picture jdoe
sudo nicl . -create /users/jdoe _shadow_passwd “”
/usr/bin/ditto -rsrc “/System/Library/User Template/English.lproj” “/User/jdoe”
/usr/sbin/chown -R 12000:20 /Users/jdoe
```

Creating a “hidden” account

- Assign or change the UID to a value less than 500 that ISN’T already being used -- it’s a good idea to number DOWN from 500.

Where do the accounts live?

You can authenticate locally or to a remote server, because your account may be...

- in the local NetInfo database
- in a remote NetInfo database
- in BSD flat files
- in an LDAP directory
- in Active Directory

What does 'being an administrator' mean from an account level?

- Membership in the “admin” group (80)
- Membership in the sudoers “group”

(/etc/sudoers)

- Unlock anyone's screen saver
- Run the Installer application
- Feel really important
- (for more, attend session M255)

What's the difference between "admin" and "wheel"

- wheel (GID 0) is like the “root” group -- so even as an admin, you’ll need to sudo to modify with these -- in other words, messing these up is really gonna cost you.
- Files are owned by the wheel group so that you can’t inadvertently modify or delete them (the use of sudo is required)

admin vs. wheel cont.

- admin group is GID 80
- Files owned by the admin group can be modified by admins without extra safeguards

Creating a group from the command line

- Create the group *newgroup* with a gid that doesn’t conflict with existing groups (*10,000-64,000*)

```
sudo nicl . -create /groups/newgroup gid 12345
```

- Disable *newgroup*’s password

```
sudo nicl . -create /groups/newgroup passwd "*"
```

- Add user *johndoe* to *newgroup*

```
sudo nicl . -merge /groups/newgroup users johndoe
```

NetInfo Database

NetInfo Database

- What is the NetInfo Database (and why should I back it up RIGHT NOW!)?

DEMO

Backing up a NetInfo Database

```
cd /var/db/netinfo/

sudo /usr/bin/nidump -r / . >
local.nidb.back
```

Restoring a “NetInfo-hosed” machine

```
cd /var/db/netinfo/

sudo /usr/bin/niload -d -r

/ local.nidb.back .
```

- Reboot `/sbin/reboot`

Okay, so what is a NetInfo Database?

The database that holds the local account information, machine configuration, and some other things commonly found in the /etc directory of other Unix systems (such as hosts and mounts)

NetInfo Database

"I don't like NetInfo - can I use flat files like any other unix OS?"

- Yes, but you shouldn’t. Apple and third-parties will expect it to be there, and need to place things there.

NetInfo Database Best Practices:

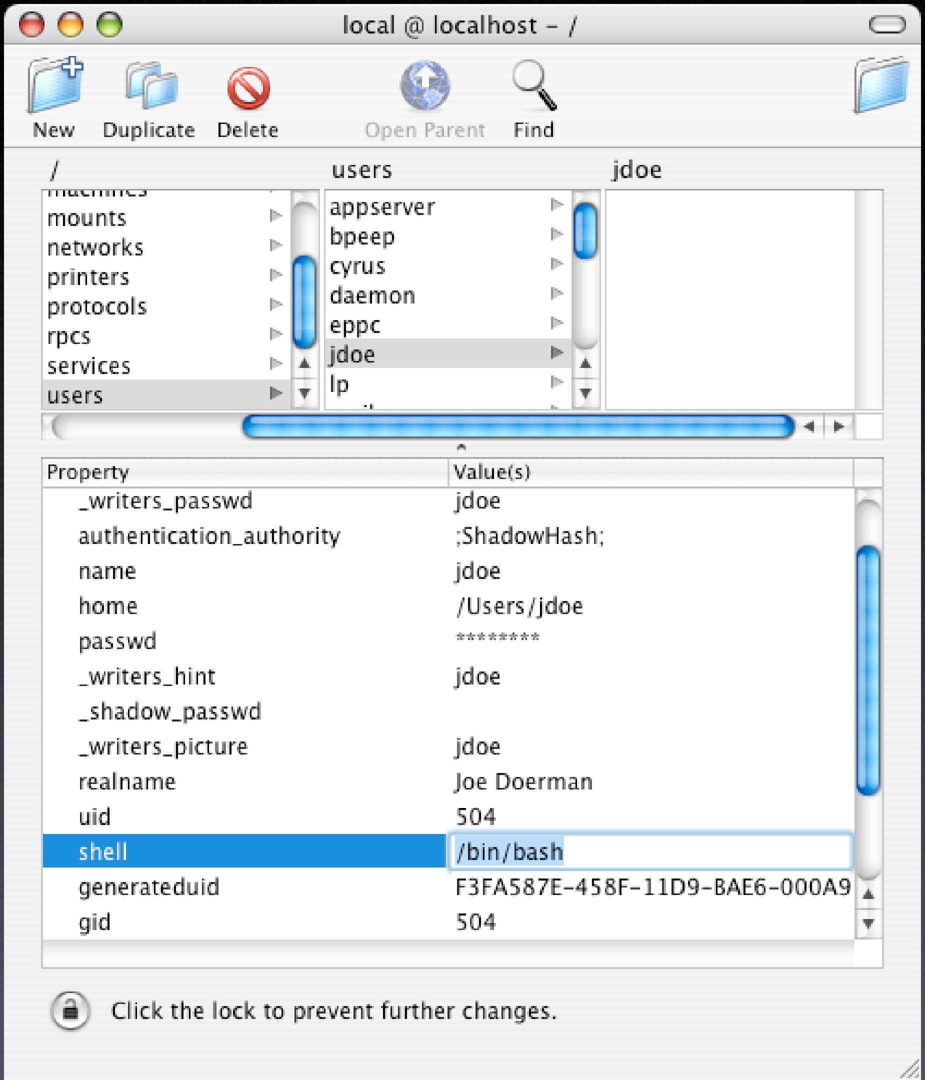
- Backup your NetInfo database before you modify it.
- Do NOT manipulate the NetInfo database with more than one tool at a time!

TOOLS

Generally speaking...

- To restrict existing access:
- Modify MCX settings through the “Limitation” tab on the Accounts preference pane, or with the “Preferences” tab in Workgroup Manager
- To open up access:
- Modify /etc/authorization *(see session M255)*

NetInfo Manager



Property	Value(s)
_writers_passwd	jdoe
authentication_authority	;ShadowHash;
name	jdoe
home	/Users/jdoe
passwd	********
_writers_hint	jdoe
_shadow_passwd	
_writers_picture	jdoe
realname	Joe Doerman
uid	504
shell	/bin/bash
generateduid	F3FA587E-458F-11D9-BAE6-000A9
gid	504

Click the lock to prevent further changes.

NetInfo Manager

What do I absolutely need the NetInfo Manager for that I can't do any other way?

- Enable and Disable root login
- (see `dsenableroot`)
- Dig deeper into the NetInfo Database
- Pretty much everything else can be done using the Workgroup Manager

Should I enable the root account?

Why?

- Feel like a cool Unix sys admin (Mac background)
- Tradition (Unix background)
- Don’t have to sudo all the time

Why Not?

- Cannot brute-force attack root account
- Encourages the use of sudo, which provides a log entry for each administrative action taken

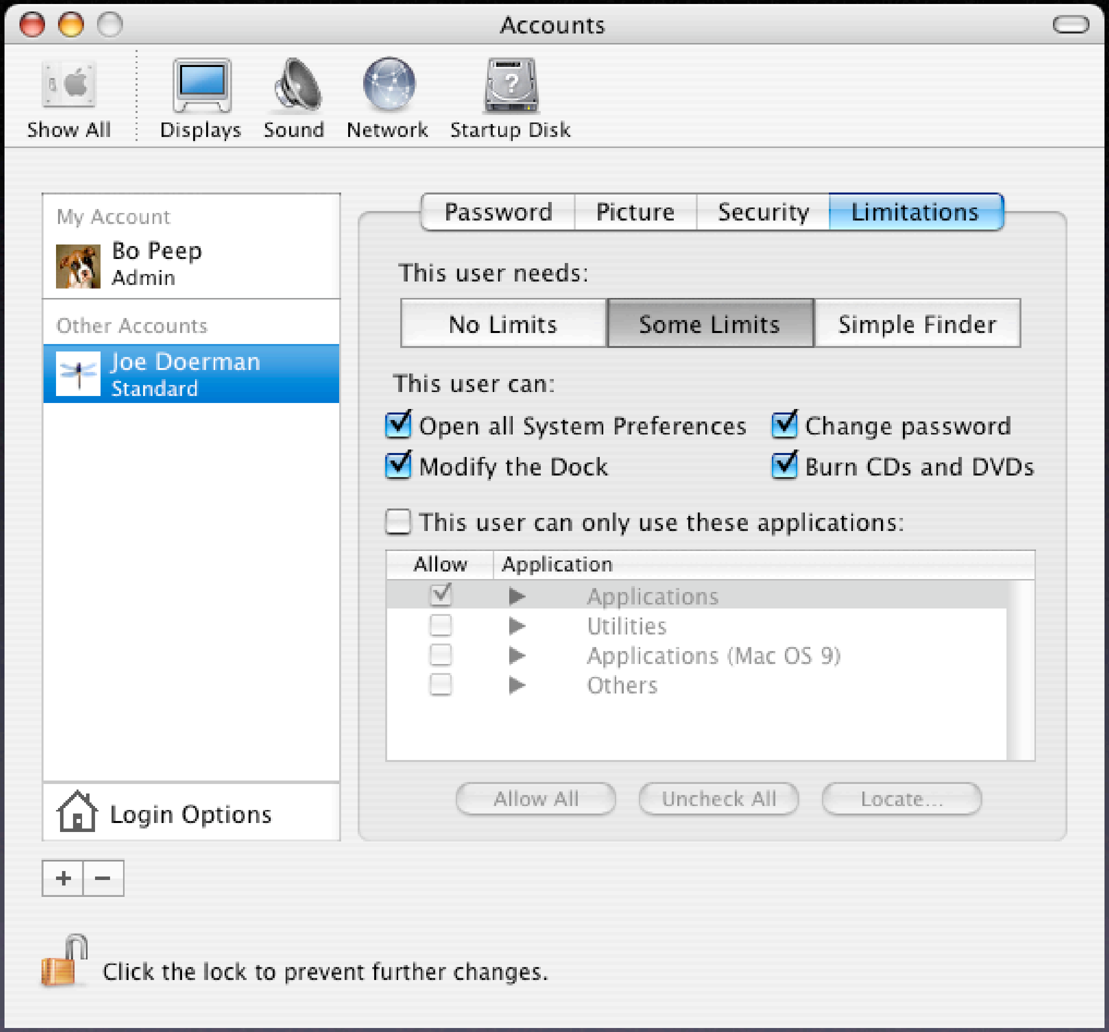
What actually happens when you enable root?

- Shadow password for root is set
- Removes `;DisabledUser;` tag, if present, from `authentication_authority` property

System Preferences Accounts Pane

System Preferences Accounts Pane

- Provides a fair amount of control over account capabilities
- That control is in big chunks...



My Account
Bo Peep
Admin

Other Accounts
Joe Doerman
Standard

Login Options

This user needs:

No Limits | **Some Limits** | Simple Finder

This user can:

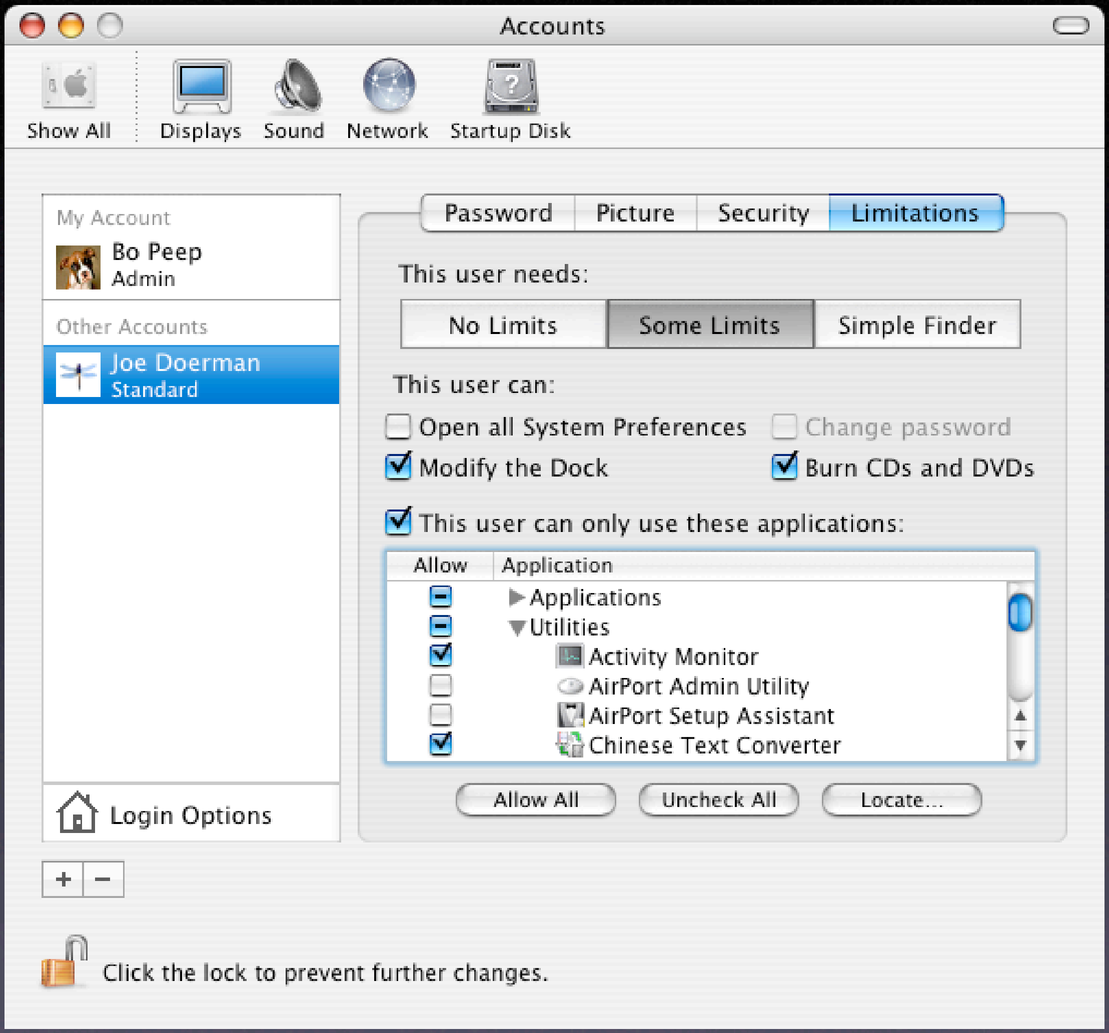
☑ Open all System Preferences ☑ Change password

☑ Modify the Dock ☑ Burn CDs and DVDs

□ This user can only use these applications:

Allow	Application
☑	▶ Applications
□	▶ Utilities
□	▶ Applications (Mac OS 9)
□	▶ Others

Click the lock to prevent further changes.



My Account

Bo Peep
Admin

Other Accounts

Joe Doerman
Standard

This user needs: No Limits [✓ Some Limits] Simple Finder

This user can:

☐ Open all System Preferences ☐ Change password

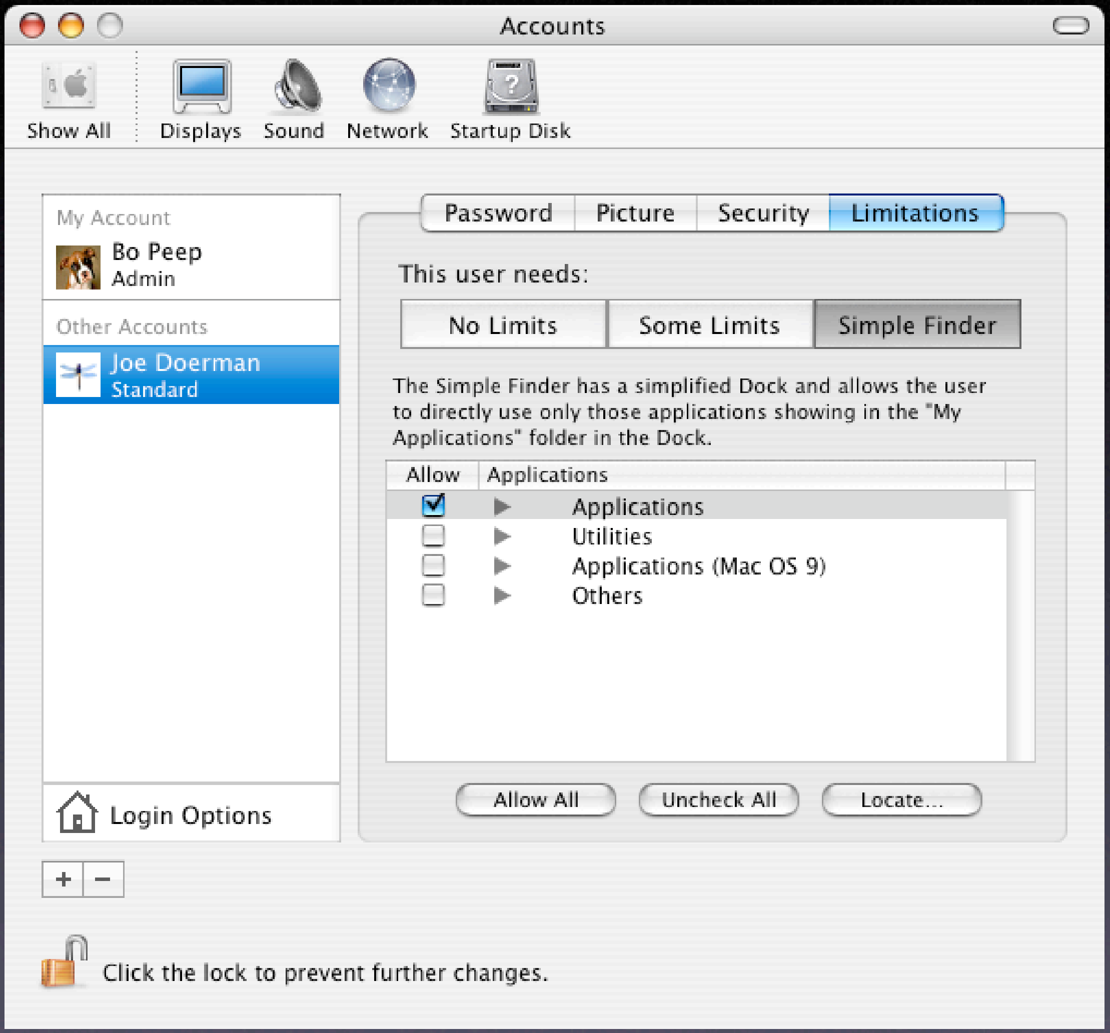
☑ Modify the Dock ☑ Burn CDs and DVDs

☑ This user can only use these applications:

Allow	Application
▬	▶ Applications
▬	▼ Utilities
☑	Activity Monitor
☐	AirPort Admin Utility
☐	AirPort Setup Assistant
☑	Chinese Text Converter

Click the lock to prevent further changes.

DEMO

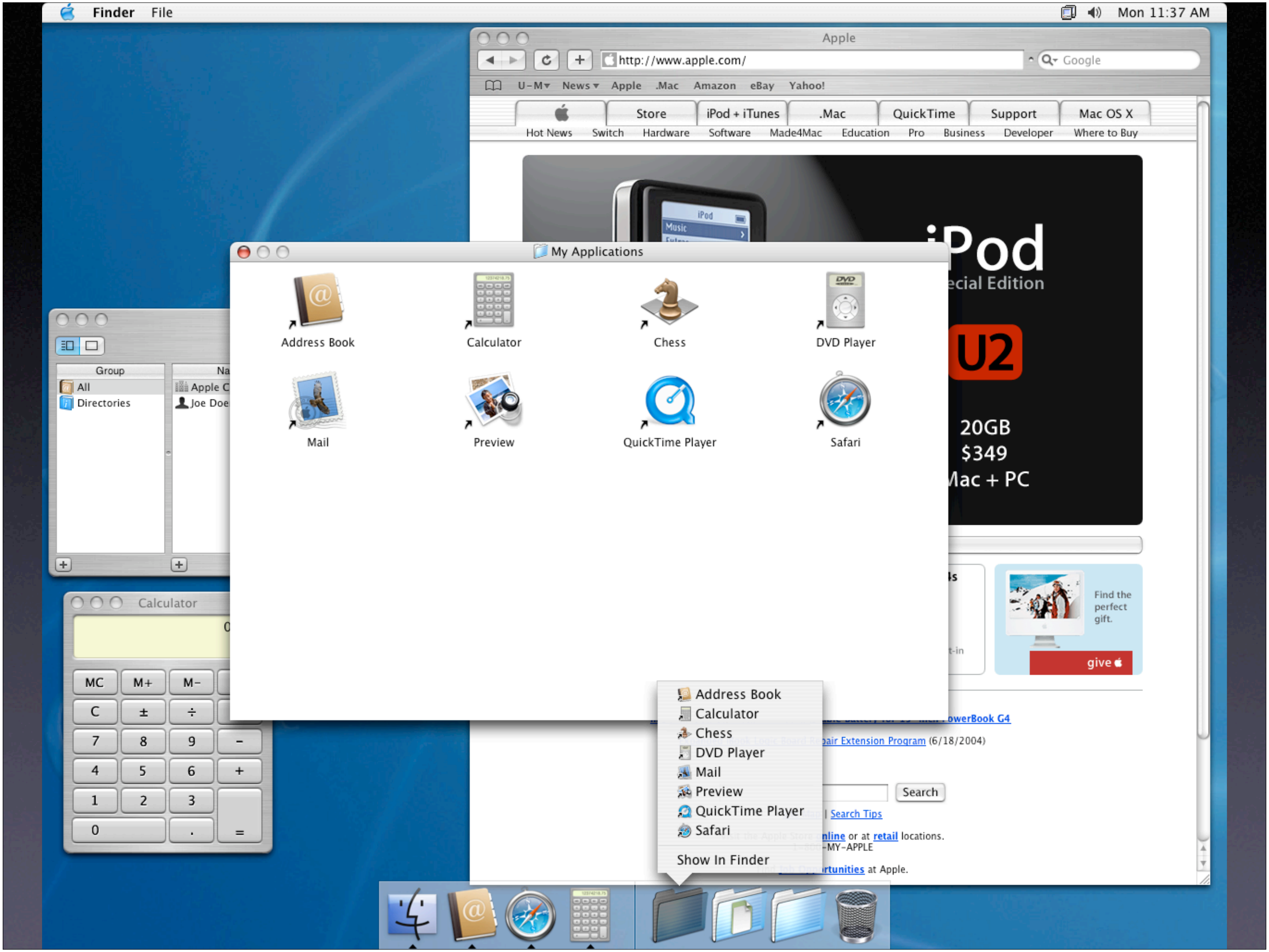


This user needs: No Limits Some Limits [✓ Simple Finder]

The Simple Finder has a simplified Dock and allows the user to directly use only those applications showing in the "My Applications" folder in the Dock.

Allow	Applications
☑	▶ Applications
□	▶ Utilities
□	▶ Applications (Mac OS 9)
□	▶ Others

Click the lock to prevent further changes.


Finder
File
Mon 11:37 AM
Apple
http://www.apple.com/
Google
U-M
News
Apple
.Mac
Amazon
eBay
Yahoo!
Store
iPod + iTunes
.Mac
QuickTime
Support
Mac OS X
Hot News
Switch
Hardware
Software
Made4Mac
Education
Pro
Business
Developer
Where to Buy
iPod
ecial Edition
U2
20GB
$349
Mac + PC
Find the perfect gift.
give
owerBook G4
air Extension Program (6/18/2004)
Search
Search Tips
nline or at retail locations.
-MY-APPLE
rtunities at Apple.
My Applications
Address Book
Calculator
Chess
DVD Player
Mail
Preview
QuickTime Player
Safari
Group
All
Directories
Na
Apple C
Joe Doe
Calculator
0
MC
M+
M−
C
±
÷
7
8
9
−
4
5
6
+
1
2
3
0
.
=
Address Book
Calculator
Chess
DVD Player
Mail
Preview
QuickTime Player
Safari
Show In Finder

Workgroup Manager

"An administrator’s dream"

...can be satisfied by MCX settings

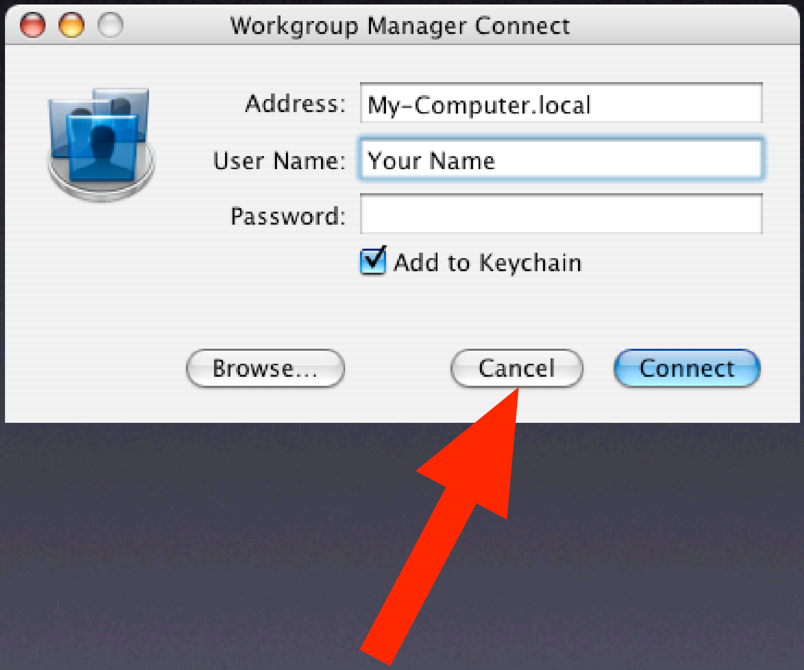
What can we do with MCX Settings?

- MCX Settings = “Managed User” Settings
- Set overriding preferences such as dock behavior, screen saver behavior, etc.
- Limit application access
- All without a server -- these are all attributes of the USER ACCOUNT!

Getting Workgroup Manager

- http://www.apple.com/downloads/macosx/apple/macosxserveradmintools.html

Connecting



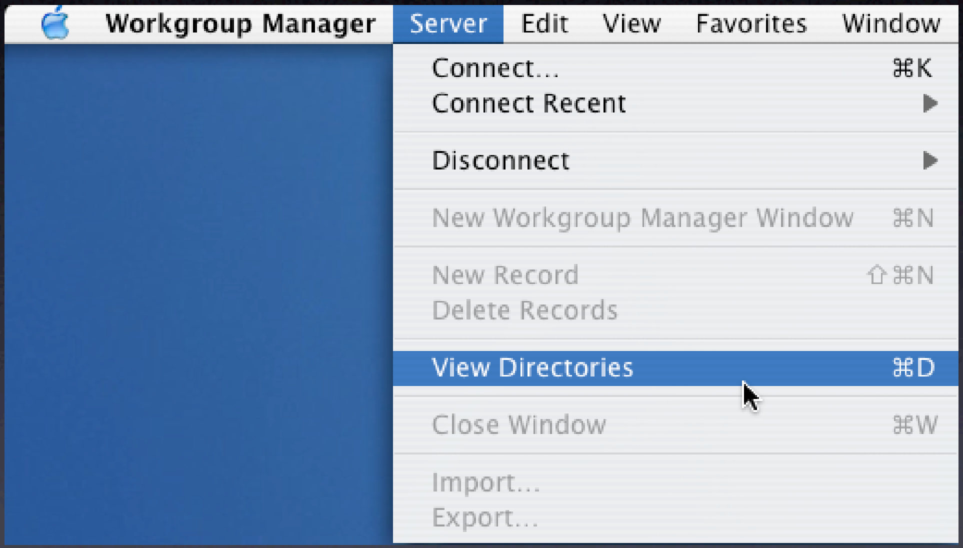
Address: My-Computer.local

User Name: Your Name

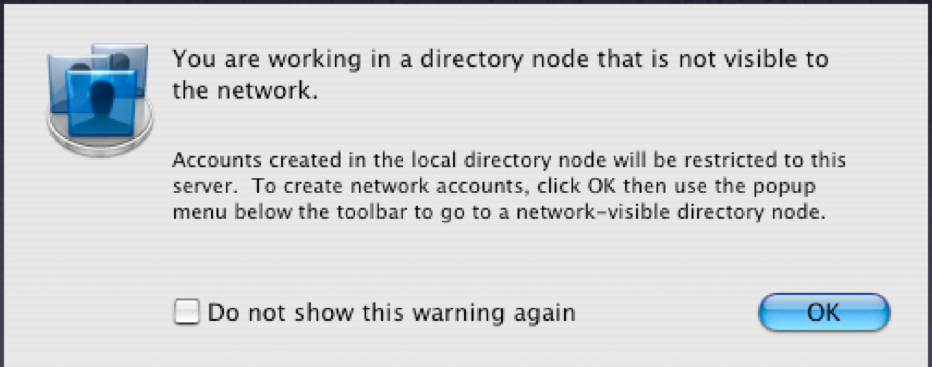
Password:

☑ Add to Keychain

Getting into YOUR NetInfo database



Whuh? Don't worry... but don't ignore, either



You are working in a directory node that is not visible to the network.

Accounts created in the local directory node will be restricted to this server. To create network accounts, click OK then use the popup menu below the toolbar to go to a network-visible directory node.

☐ Do not show this warning again

Creating a group from the command line

- Create the group *newgroup* with a gid that doesn’t conflict with existing groups (*10,000-64,000*)

```
sudo nicl . -create /groups/newgroup gid 12345
```

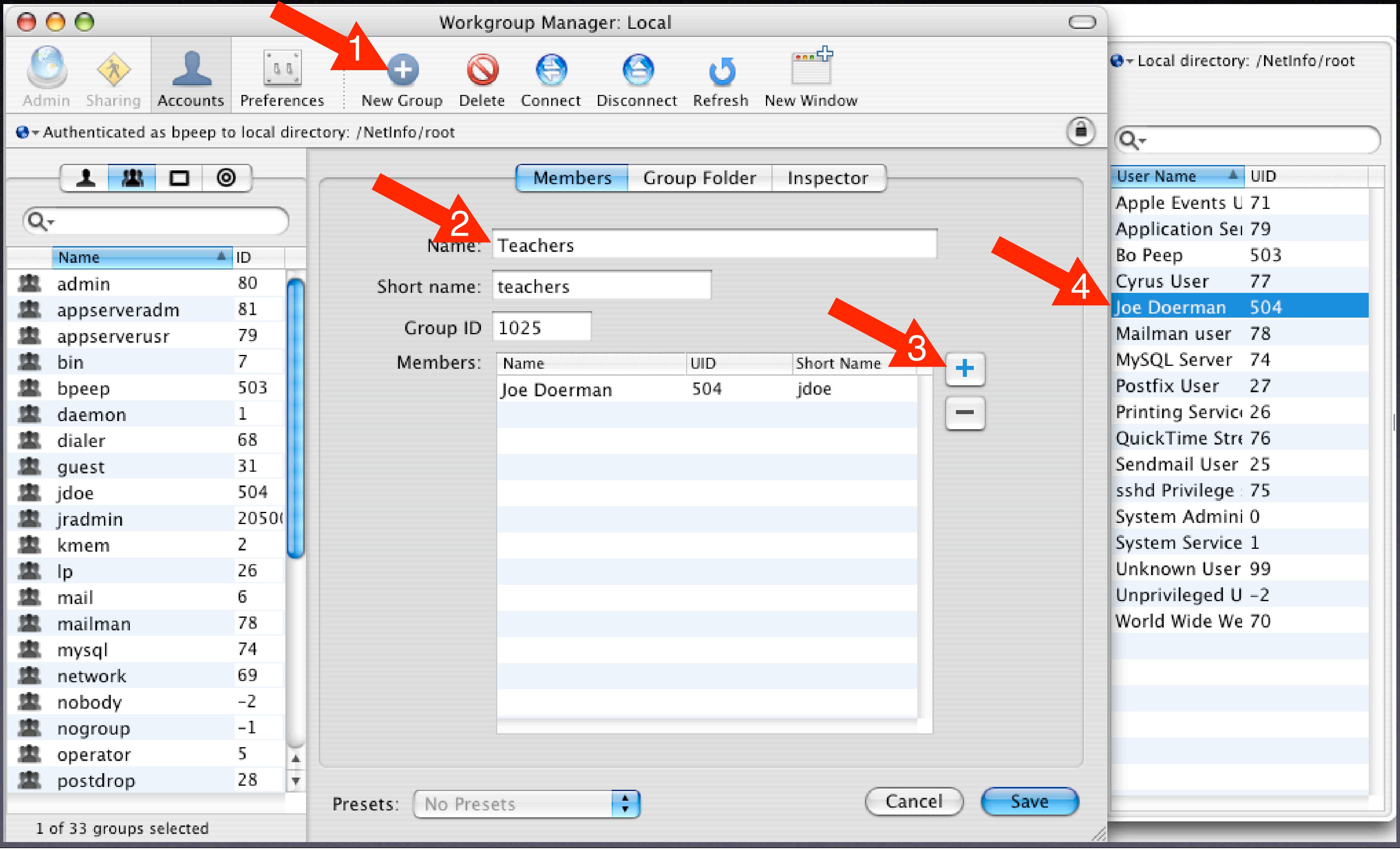
- Disable *newgroup*’s password

```
sudo nicl . -create /groups/newgroup passwd "*"
```

- Add user *johndoe* to *newgroup*

```
sudo nicl . -merge /groups/newgroup users johndoe
```

Creating a group in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
admin	80
appserveradm	81
appserverusr	79
bin	7
bpeep	503
daemon	1
dialer	68
guest	31
jdoe	504
jradmin	2050(
kmem	2
lp	26
mail	6
mailman	78
mysql	74
network	69
nobody	-2
nogroup	-1
operator	5
postdrop	28

1 of 33 groups selected

Name: Teachers

Short name: teachers

Group ID 1025

Members:

Name	UID	Short Name
Joe Doerman	504	jdoe

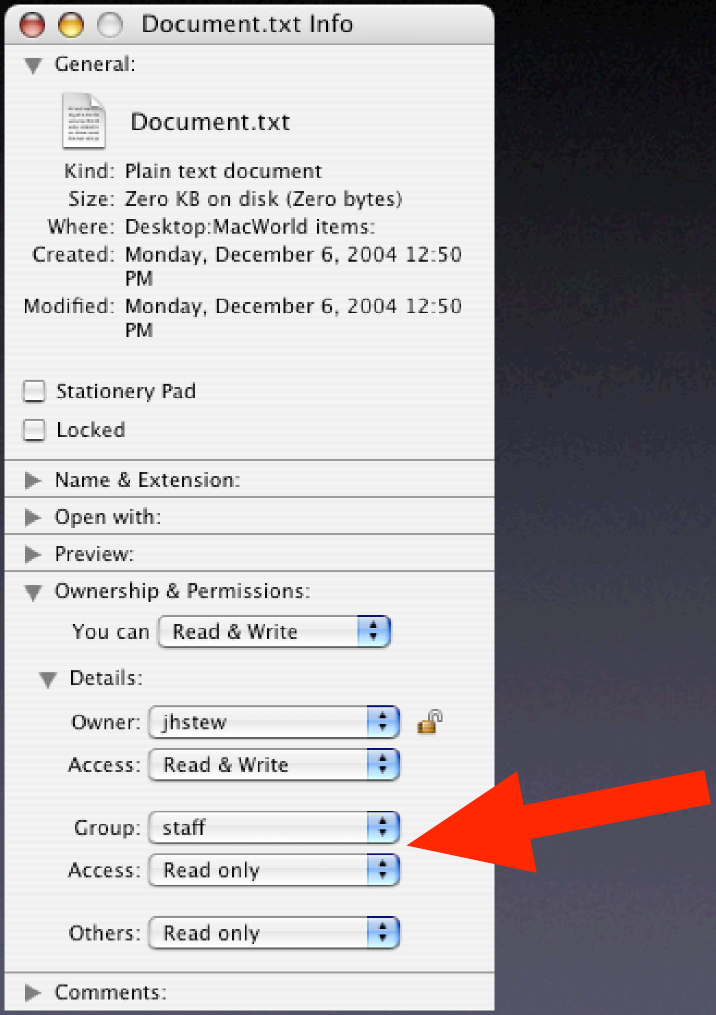
Presets: No Presets

Local directory: /NetInfo/root

User Name	UID
Apple Events U	71
Application Sei	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Servic	26
QuickTime Stre	76
Sendmail User	25
sshd Privilege	75
System Admini	0
System Service	1
Unknown User	99
Unprivileged U	-2
World Wide We	70

Create Groups

- For file access or refining authorization policies *(see session M255)*
- You can set group ownership through the Finder



Document.txt Info

▼ General:

Document.txt

Kind: Plain text document
Size: Zero KB on disk (Zero bytes)
Where: Desktop:MacWorld items:
Created: Monday, December 6, 2004 12:50 PM
Modified: Monday, December 6, 2004 12:50 PM

□ Stationery Pad
□ Locked

▶ Name & Extension:
▶ Open with:
▶ Preview:
▼ Ownership & Permissions:

You can: Read & Write

▼ Details:

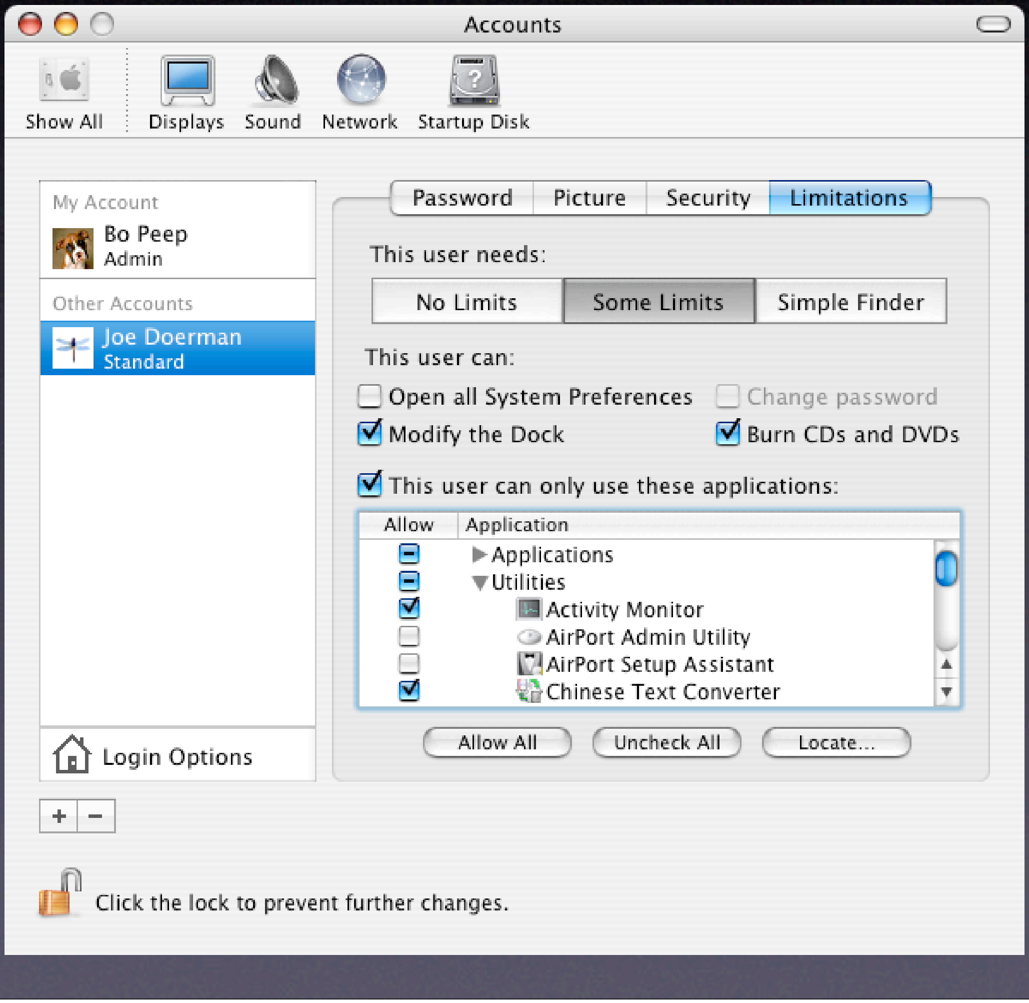
Owner: jhstew
Access: Read & Write

Group: staff
Access: Read only

Others: Read only

▶ Comments:

Application Limitations in System Preferences



My Account
Bo Peep
Admin

Other Accounts
Joe Doerman
Standard

This user needs:

No Limits | **Some Limits** | Simple Finder

This user can:

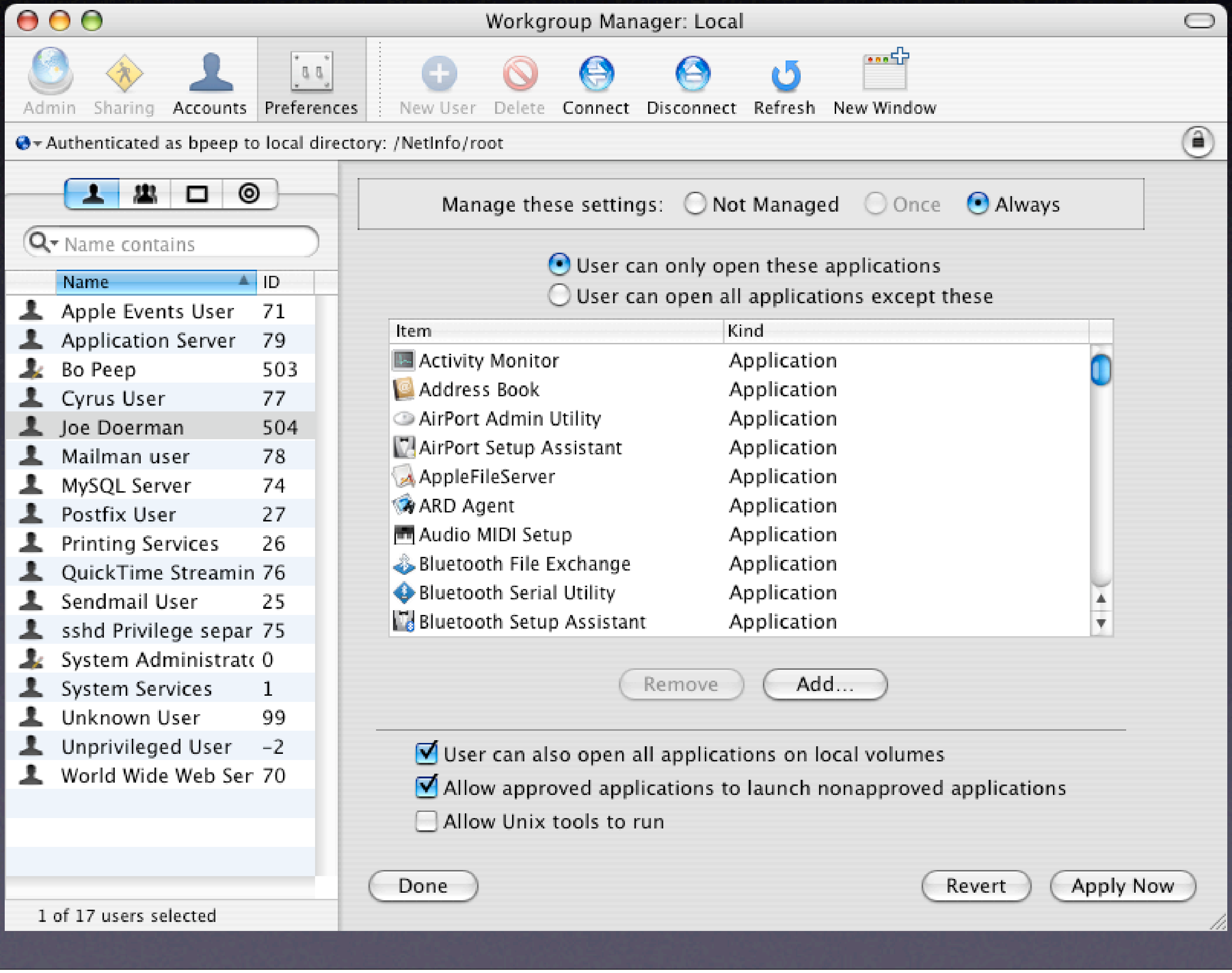
□ Open all System Preferences   □ Change password
☑ Modify the Dock   ☑ Burn CDs and DVDs

☑ This user can only use these applications:

Allow	Application
⊟	▶ Applications
⊟	▼ Utilities
☑	Activity Monitor
□	AirPort Admin Utility
□	AirPort Setup Assistant
☑	Chinese Text Converter

Click the lock to prevent further changes.

Application Limitations in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

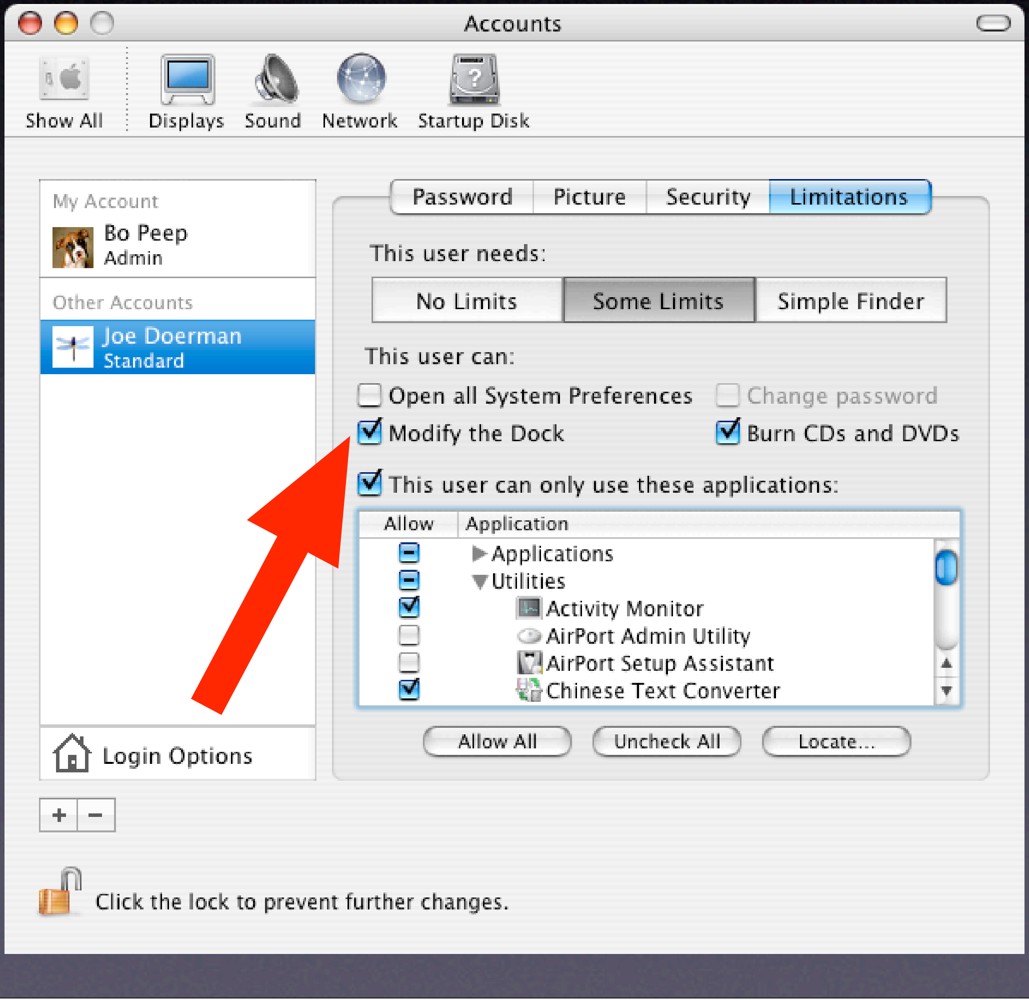
Manage these settings: ○ Not Managed ○ Once ● Always

● User can only open these applications
○ User can open all applications except these

Item	Kind
Activity Monitor	Application
Address Book	Application
AirPort Admin Utility	Application
AirPort Setup Assistant	Application
AppleFileServer	Application
ARD Agent	Application
Audio MIDI Setup	Application
Bluetooth File Exchange	Application
Bluetooth Serial Utility	Application
Bluetooth Setup Assistant	Application

☑ User can also open all applications on local volumes
☑ Allow approved applications to launch nonapproved applications
☐ Allow Unix tools to run

Controlling the Dock in System Preferences



My Account

Bo Peep
Admin

Other Accounts

Joe Doerman
Standard

This user needs:

No Limits | [✓ Some Limits] | Simple Finder

This user can:

☐ Open all System Preferences ☐ Change password

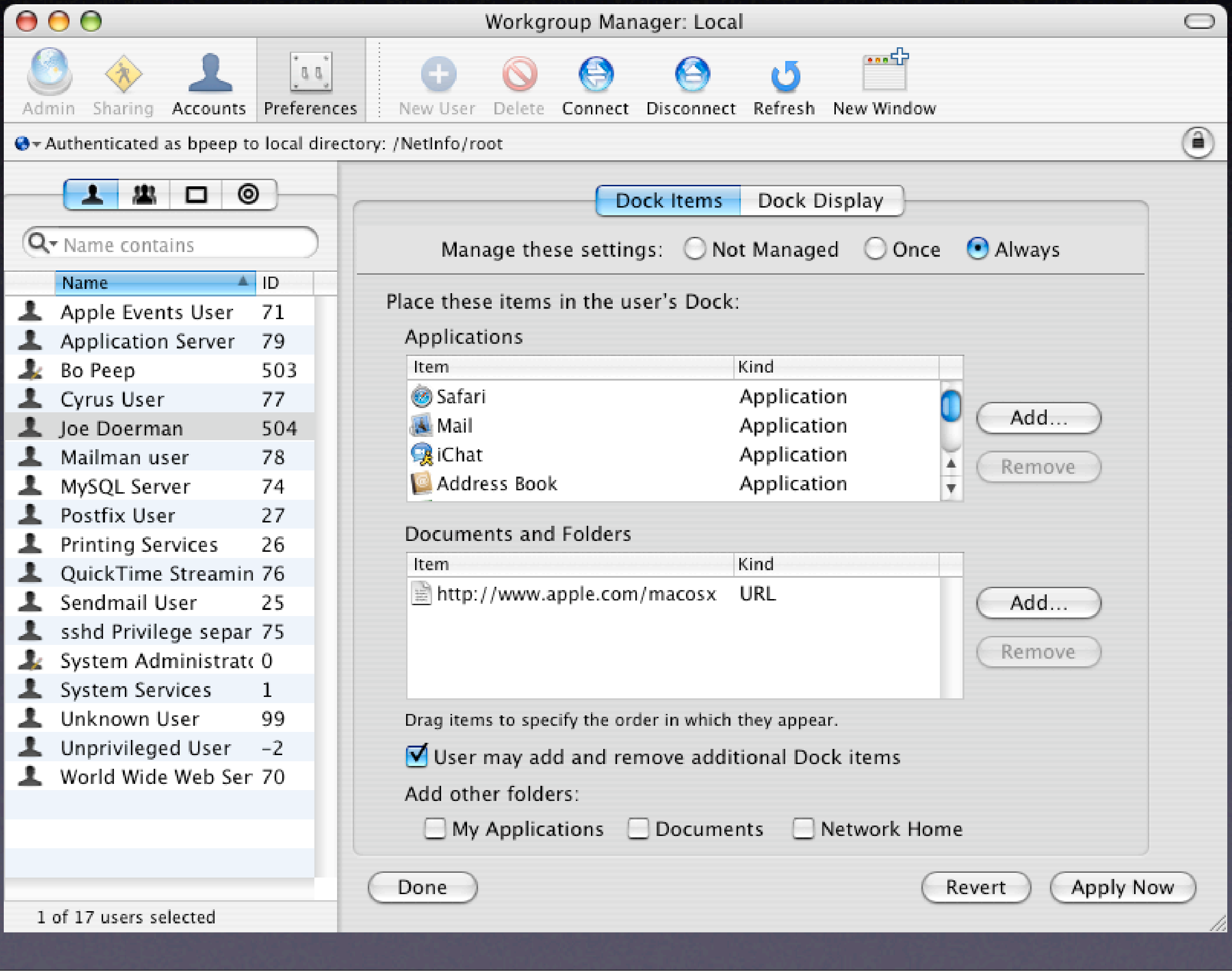
☑ Modify the Dock ☑ Burn CDs and DVDs

☑ This user can only use these applications:

Allow	Application
⊟	▶ Applications
⊟	▼ Utilities
☑	Activity Monitor
☐	AirPort Admin Utility
☐	AirPort Setup Assistant
☑	Chinese Text Converter

Click the lock to prevent further changes.

Controlling the Dock in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

Place these items in the user's Dock:

Applications

Item	Kind
Safari	Application
Mail	Application
iChat	Application
Address Book	Application

Documents and Folders

Item	Kind
http://www.apple.com/macosx	URL

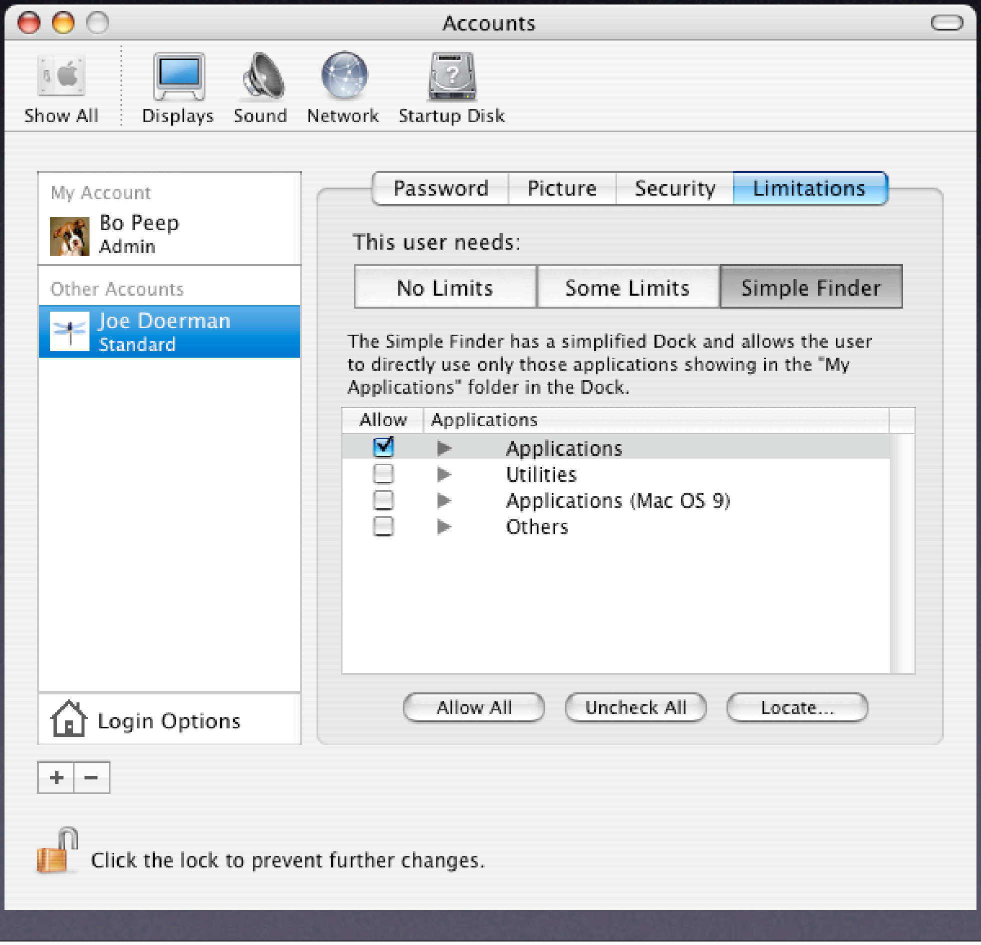
Drag items to specify the order in which they appear.

☑ User may add and remove additional Dock items

Add other folders:

□ My Applications □ Documents □ Network Home

Simple Finder in System Preferences



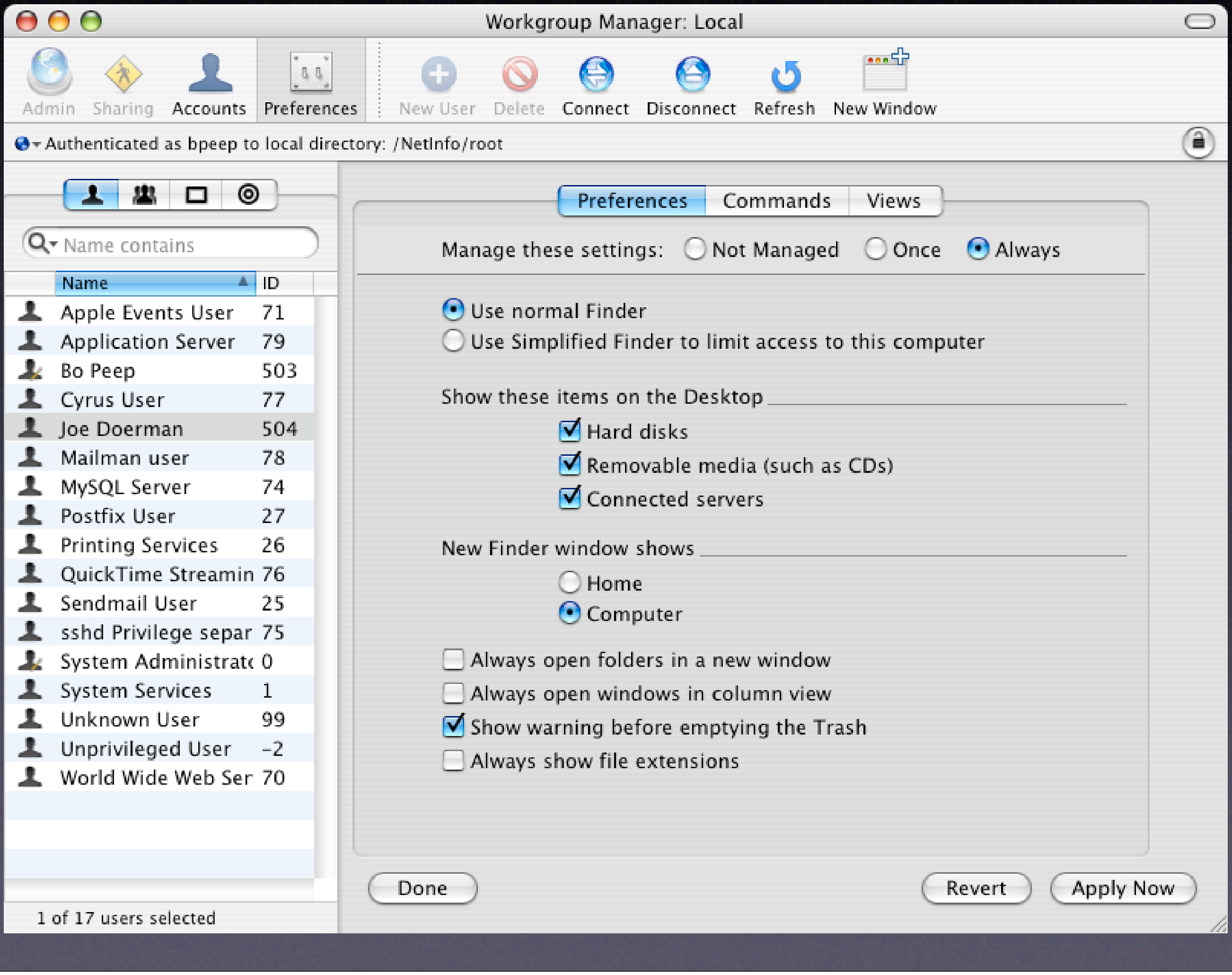
This user needs: Simple Finder

The Simple Finder has a simplified Dock and allows the user to directly use only those applications showing in the "My Applications" folder in the Dock.

Allow	Applications
☑	▶ Applications
□	▶ Utilities
□	▶ Applications (Mac OS 9)
□	▶ Others

Click the lock to prevent further changes.

Simple Finder in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administrat	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

● Use normal Finder
○ Use Simplified Finder to limit access to this computer

Show these items on the Desktop

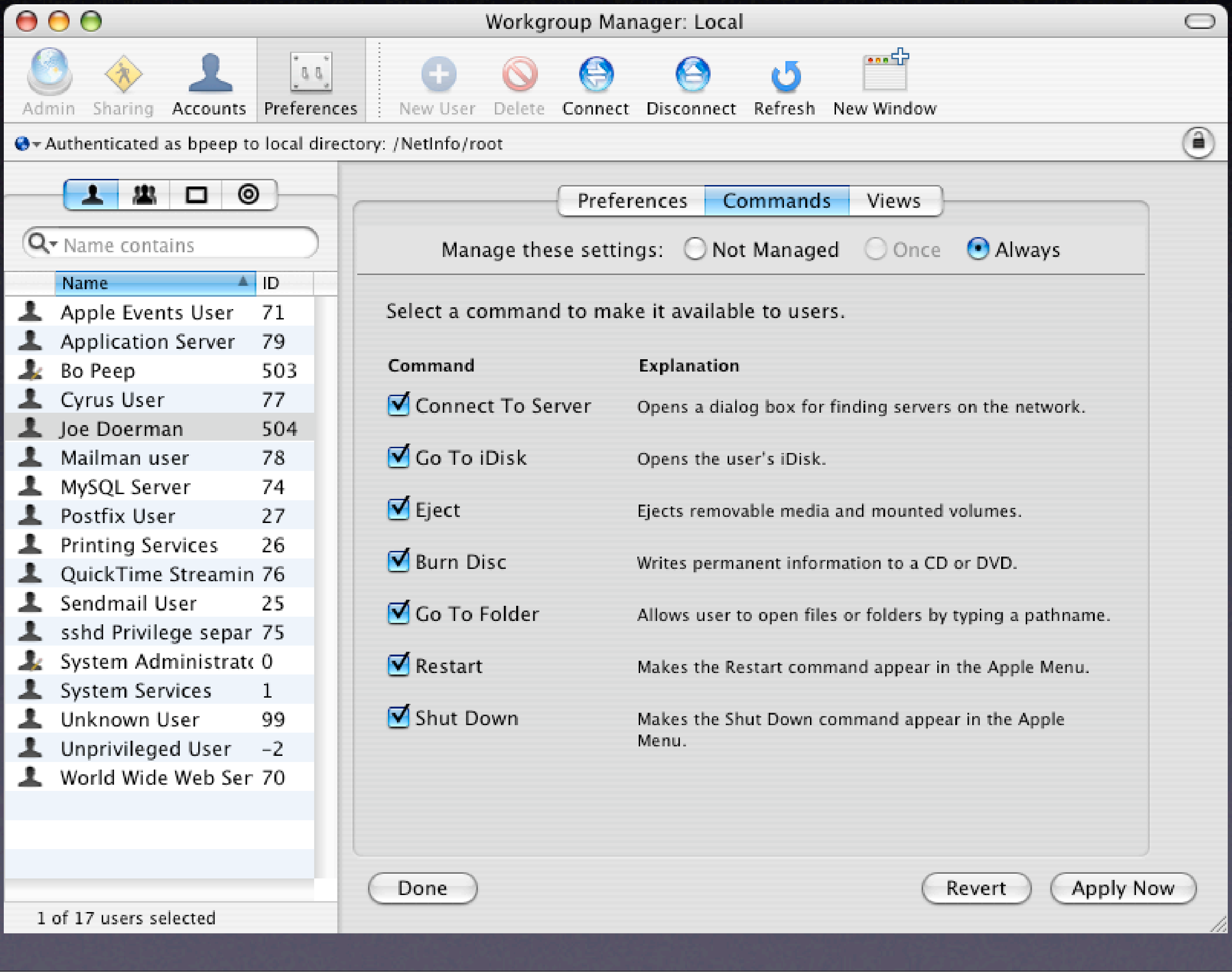
☑ Hard disks
☑ Removable media (such as CDs)
☑ Connected servers

New Finder window shows

○ Home
● Computer

□ Always open folders in a new window
□ Always open windows in column view
☑ Show warning before emptying the Trash
□ Always show file extensions

Limiting Finder Menus



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

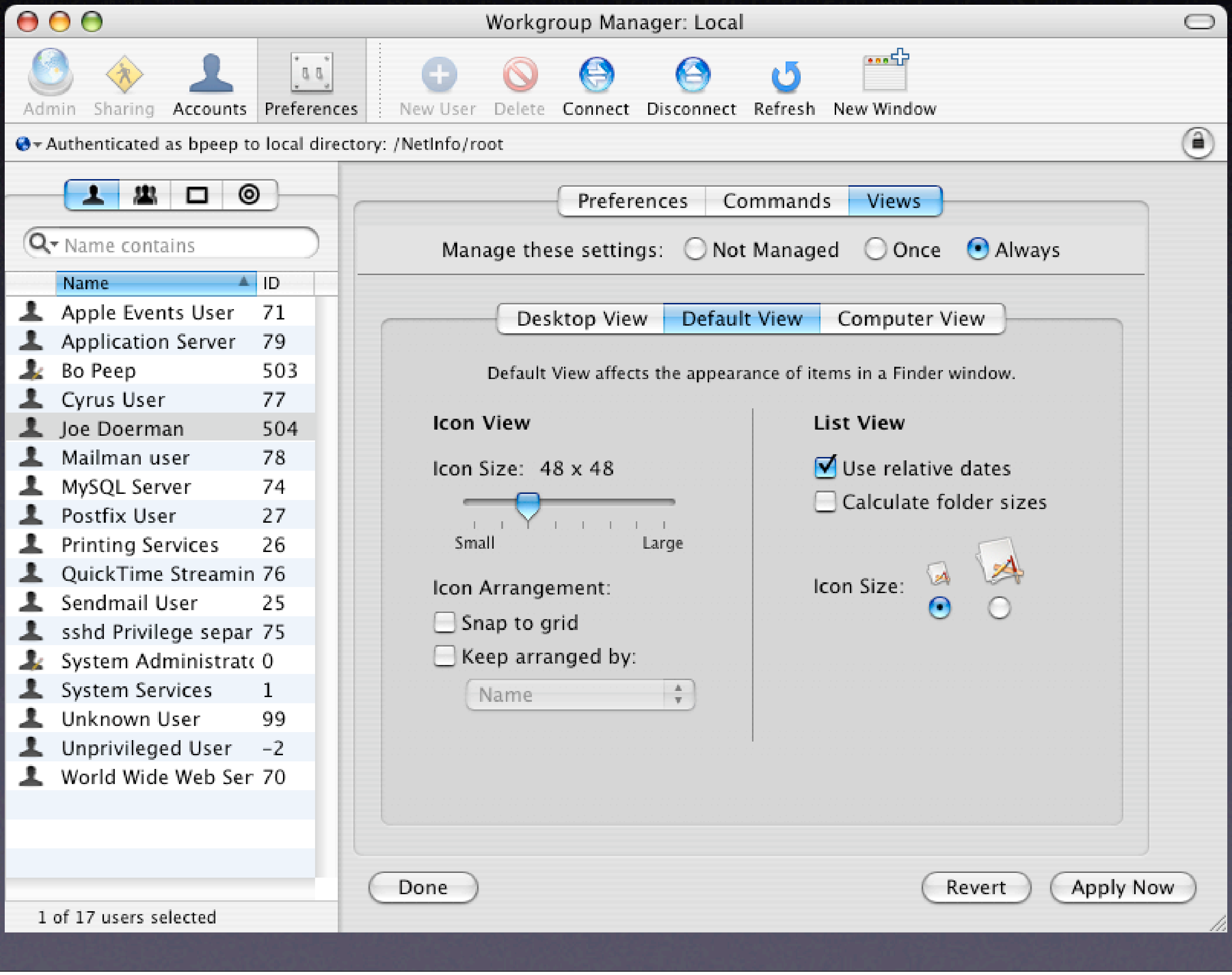
1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

Select a command to make it available to users.

Command	Explanation
☑ Connect To Server	Opens a dialog box for finding servers on the network.
☑ Go To iDisk	Opens the user's iDisk.
☑ Eject	Ejects removable media and mounted volumes.
☑ Burn Disc	Writes permanent information to a CD or DVD.
☑ Go To Folder	Allows user to open files or folders by typing a pathname.
☑ Restart	Makes the Restart command appear in the Apple Menu.
☑ Shut Down	Makes the Shut Down command appear in the Apple Menu.

Defining Finder Views



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

Default View affects the appearance of items in a Finder window.

Icon View

Icon Size: 48 x 48

Icon Arrangement:

□ Snap to grid

□ Keep arranged by: Name

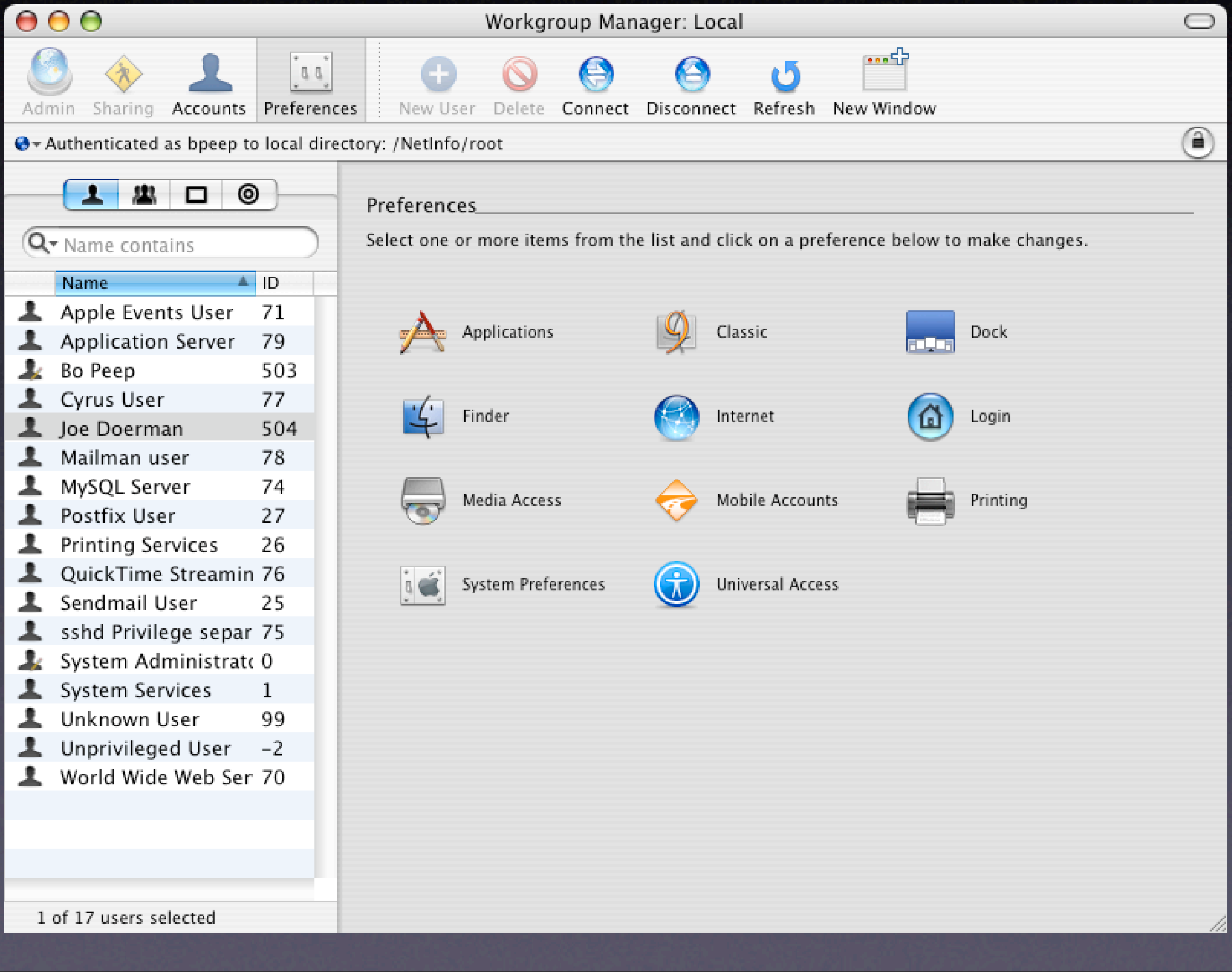
List View

☑ Use relative dates

□ Calculate folder sizes

Icon Size: ● ○

The Preferences Overview



Authenticated as bpeep to local directory: /NetInfo/root

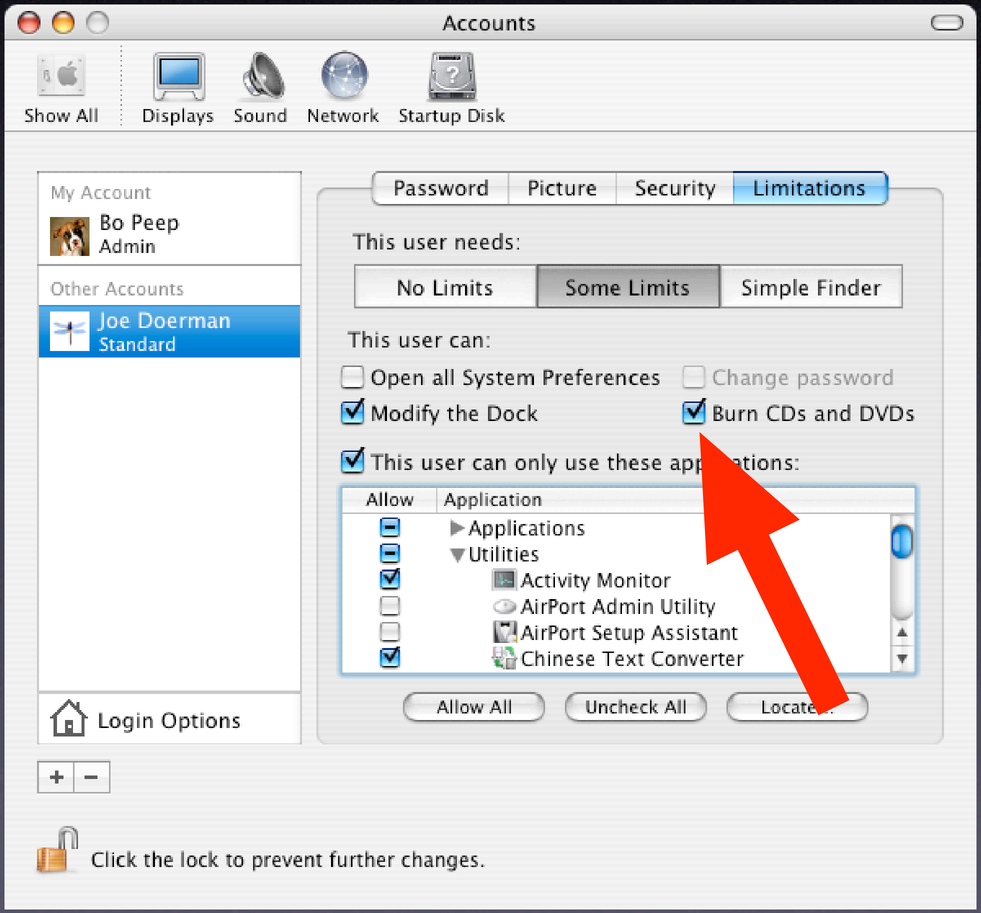
Preferences

Select one or more items from the list and click on a preference below to make changes.

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Disk Media in System Preferences



My Account
Bo Peep
Admin

Other Accounts
Joe Doerman
Standard

Login Options

This user needs: No Limits [✓ Some Limits] Simple Finder

This user can:

☐ Open all System Preferences ☐ Change password

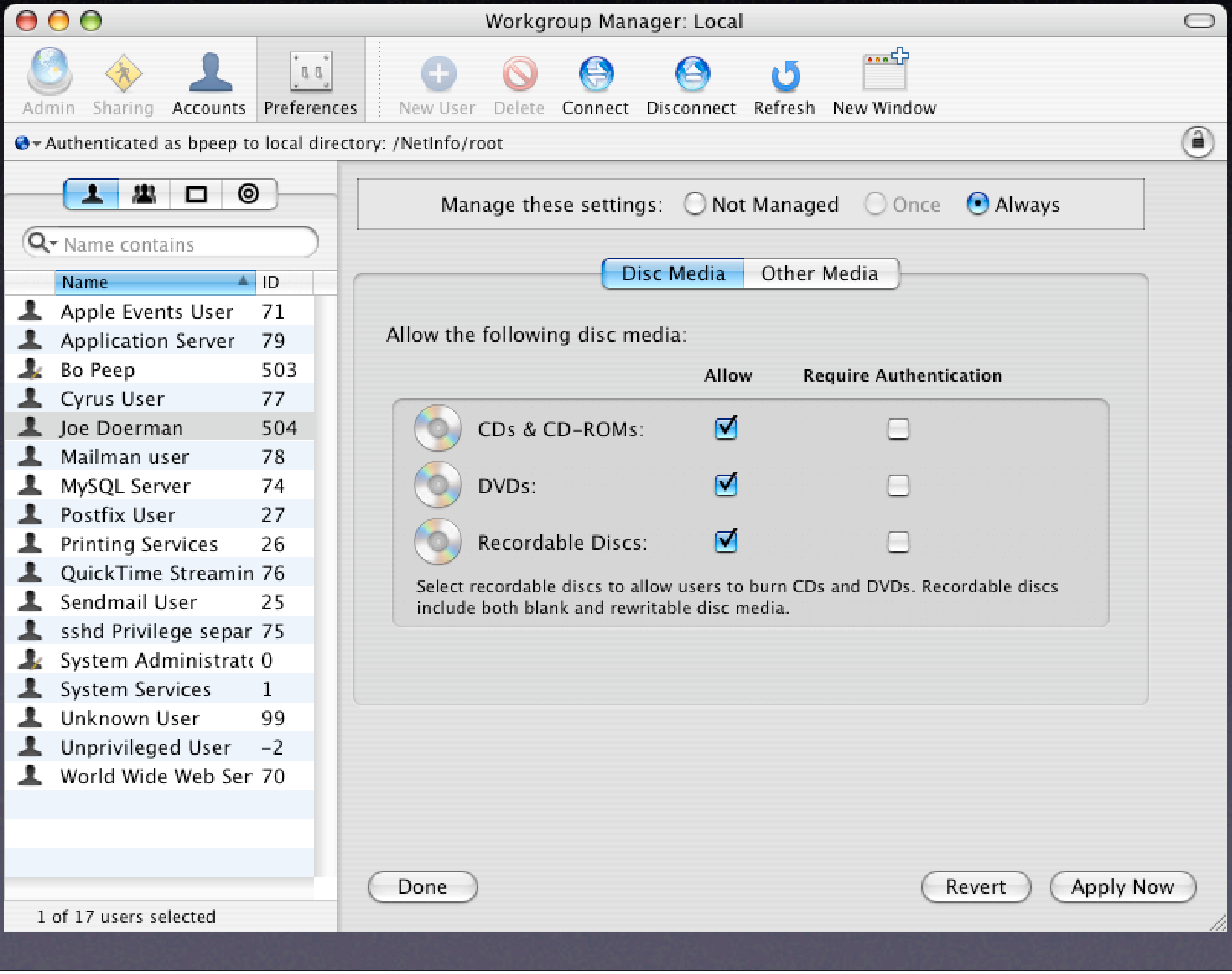
☑ Modify the Dock ☑ Burn CDs and DVDs

☑ This user can only use these app ations:

Allow	Application
⊟	▶ Applications
⊟	▼ Utilities
☑	Activity Monitor
☐	AirPort Admin Utility
☐	AirPort Setup Assistant
☑	Chinese Text Converter

Click the lock to prevent further changes.

Disk Media in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

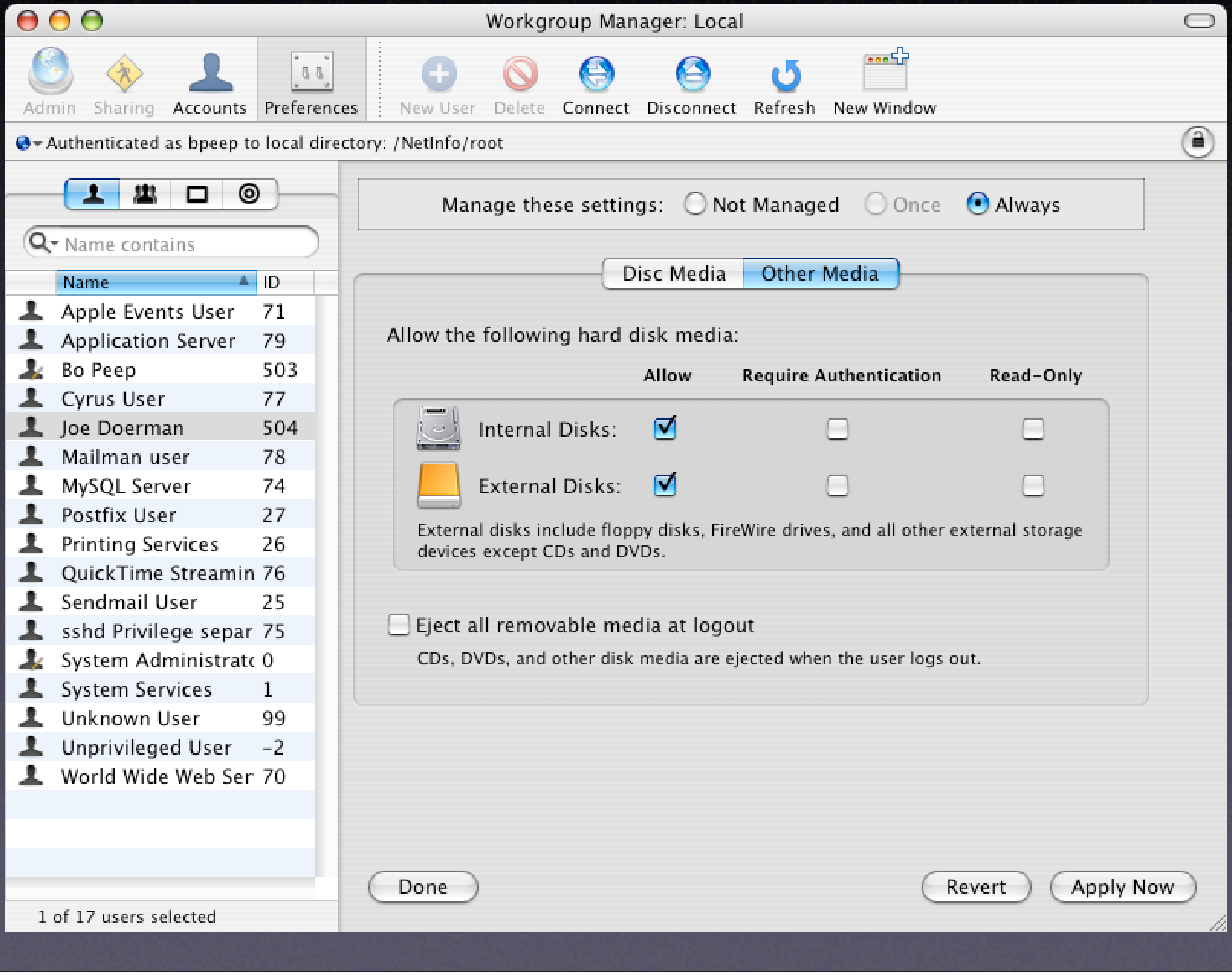
Manage these settings: ○ Not Managed ○ Once ● Always

Allow the following disc media:

	Allow	Require Authentication
CDs & CD-ROMs:	☑	□
DVDs:	☑	□
Recordable Discs:	☑	□

Select recordable discs to allow users to burn CDs and DVDs. Recordable discs include both blank and rewritable disc media.

Other Media



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

Disc Media | Other Media

Allow the following hard disk media:

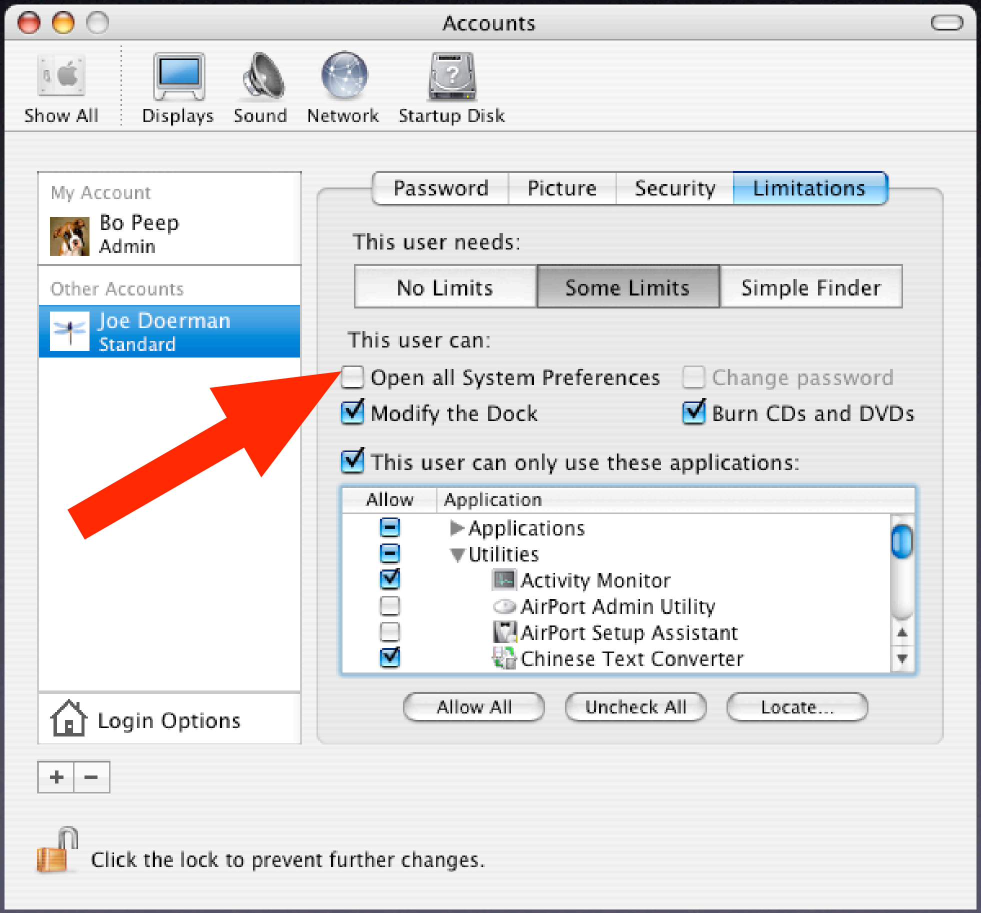
	Allow	Require Authentication	Read-Only
Internal Disks:	☑	□	□
External Disks:	☑	□	□

External disks include floppy disks, FireWire drives, and all other external storage devices except CDs and DVDs.

□ Eject all removable media at logout

CDs, DVDs, and other disk media are ejected when the user logs out.

Controlling Preferences in System Preferences



This user needs: No Limits [✓ Some Limits] Simple Finder

This user can:

□ Open all System Preferences □ Change password

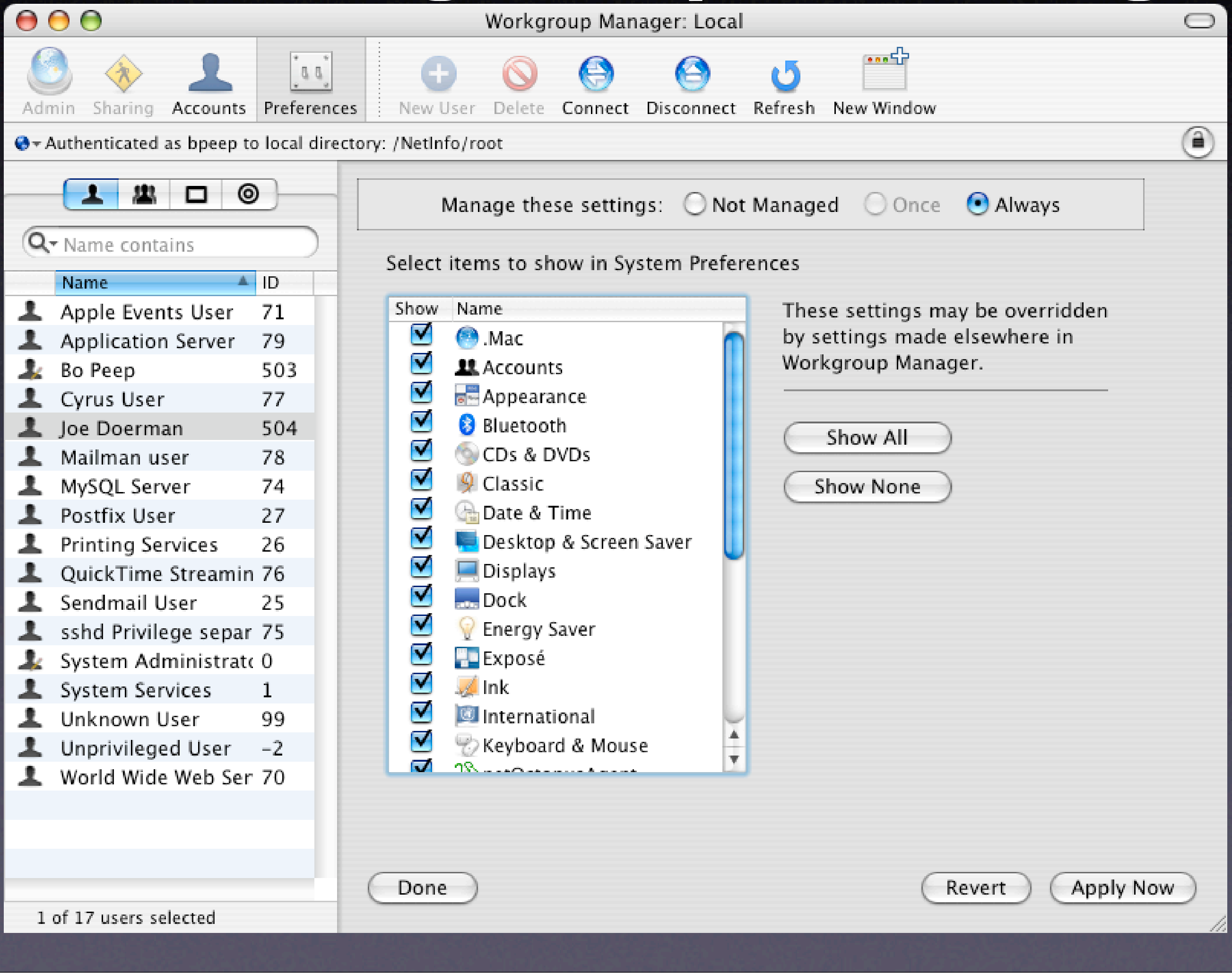
☑ Modify the Dock ☑ Burn CDs and DVDs

☑ This user can only use these applications:

Allow	Application
−	▶ Applications
−	▼ Utilities
☑	Activity Monitor
□	AirPort Admin Utility
□	AirPort Setup Assistant
☑	Chinese Text Converter

Click the lock to prevent further changes.

Controlling Preferences in Workgroup Manager



Authenticated as bpeep to local directory: /NetInfo/root

Name contains

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administrato	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Manage these settings: ○ Not Managed ○ Once ● Always

Select items to show in System Preferences

Show	Name
☑	.Mac
☑	Accounts
☑	Appearance
☑	Bluetooth
☑	CDs & DVDs
☑	Classic
☑	Date & Time
☑	Desktop & Screen Saver
☑	Displays
☑	Dock
☑	Energy Saver
☑	Exposé
☑	Ink
☑	International
☑	Keyboard & Mouse

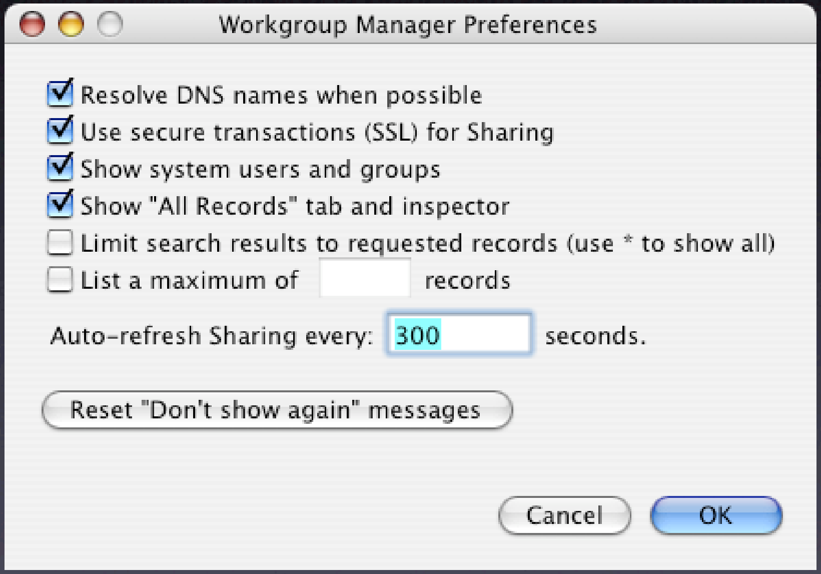
These settings may be overridden by settings made elsewhere in Workgroup Manager.

The Inspector

- The inspector button lets you view the NetInfo database in a way that looks like the NetInfo Manager

Getting it going

- Start Workgroup Manager, cancel the ‘connect”dialog and open the Workgroup Manager Preferences
- Select ‘Show system users and groups’
- Select ‘Show “All Records” tab and inspector’
- Ignore subsequent warning message own peril...



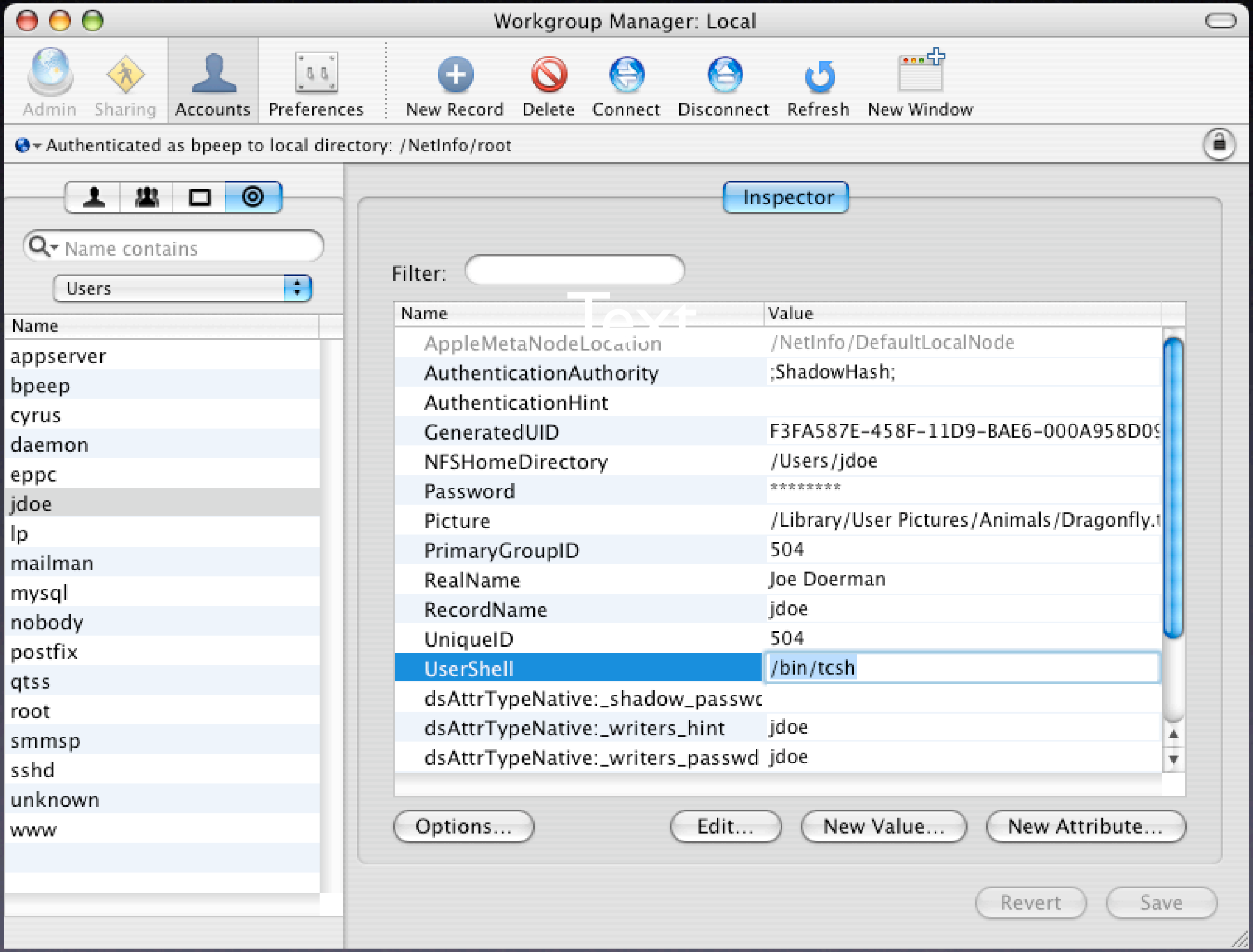
Workgroup Manager Preferences

☑ Resolve DNS names when possible
☑ Use secure transactions (SSL) for Sharing
☑ Show system users and groups
☑ Show "All Records" tab and inspector
□ Limit search results to requested records (use * to show all)
□ List a maximum of ____ records

Auto-refresh Sharing every: 300 seconds.

Reset "Don't show again" messages
Cancel
OK

The Inspector



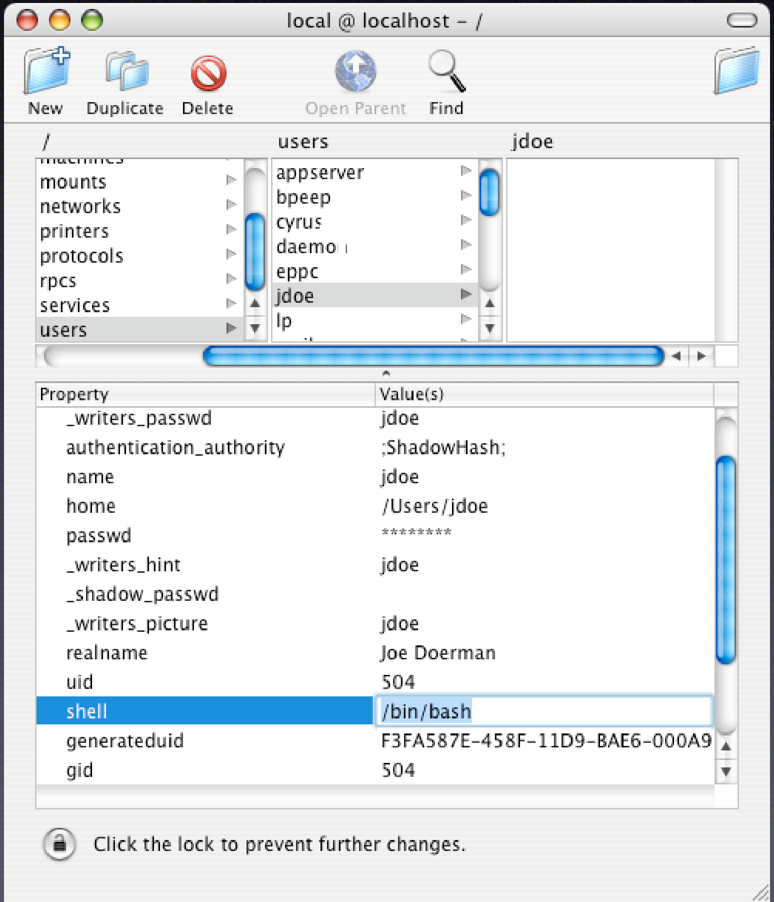
Authenticated as bpeep to local directory: /NetInfo/root

Name
appserver
bpeep
cyrus
daemon
eppc
jdoe
lp
mailman
mysql
nobody
postfix
qtss
root
smmsp
sshd
unknown
www

Filter:

Name	Value
AppleMetaNodeLocation	/NetInfo/DefaultLocalNode
AuthenticationAuthority	;ShadowHash;
AuthenticationHint	
GeneratedUID	F3FA587E-458F-11D9-BAE6-000A958D0!
NFSHomeDirectory	/Users/jdoe
Password	********
Picture	/Library/User Pictures/Animals/Dragonfly.t
PrimaryGroupID	504
RealName	Joe Doerman
RecordName	jdoe
UniqueID	504
UserShell	/bin/tcsh
dsAttrTypeNative:_shadow_passwc	
dsAttrTypeNative:_writers_hint	jdoe
dsAttrTypeNative:_writers_passwd	jdoe

...as compared to the NetInfo Manager



Property	Value(s)
_writers_passwd	jdoe
authentication_authority	;ShadowHash;
name	jdoe
home	/Users/jdoe
passwd	********
_writers_hint	jdoe
_shadow_passwd	
_writers_picture	jdoe
realname	Joe Doerman
uid	504
shell	/bin/bash
generateduid	F3FA587E-458F-11D9-BAE6-000A9
gid	504

Click the lock to prevent further changes.

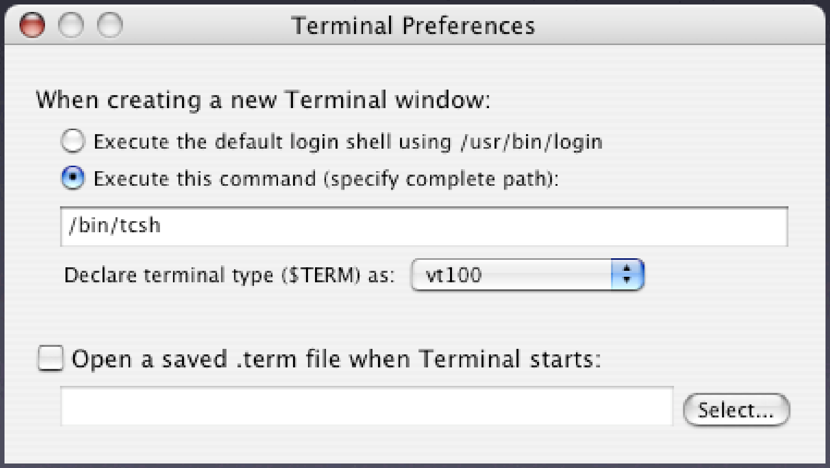
Example Uses

So what are some useful things I can do with my new-found powers?

DEMO

Set the Default Shell

- Users can also do this on their own through the Terminal Preferences or by using the `chsh` command.



Terminal Preferences

When creating a new Terminal window:

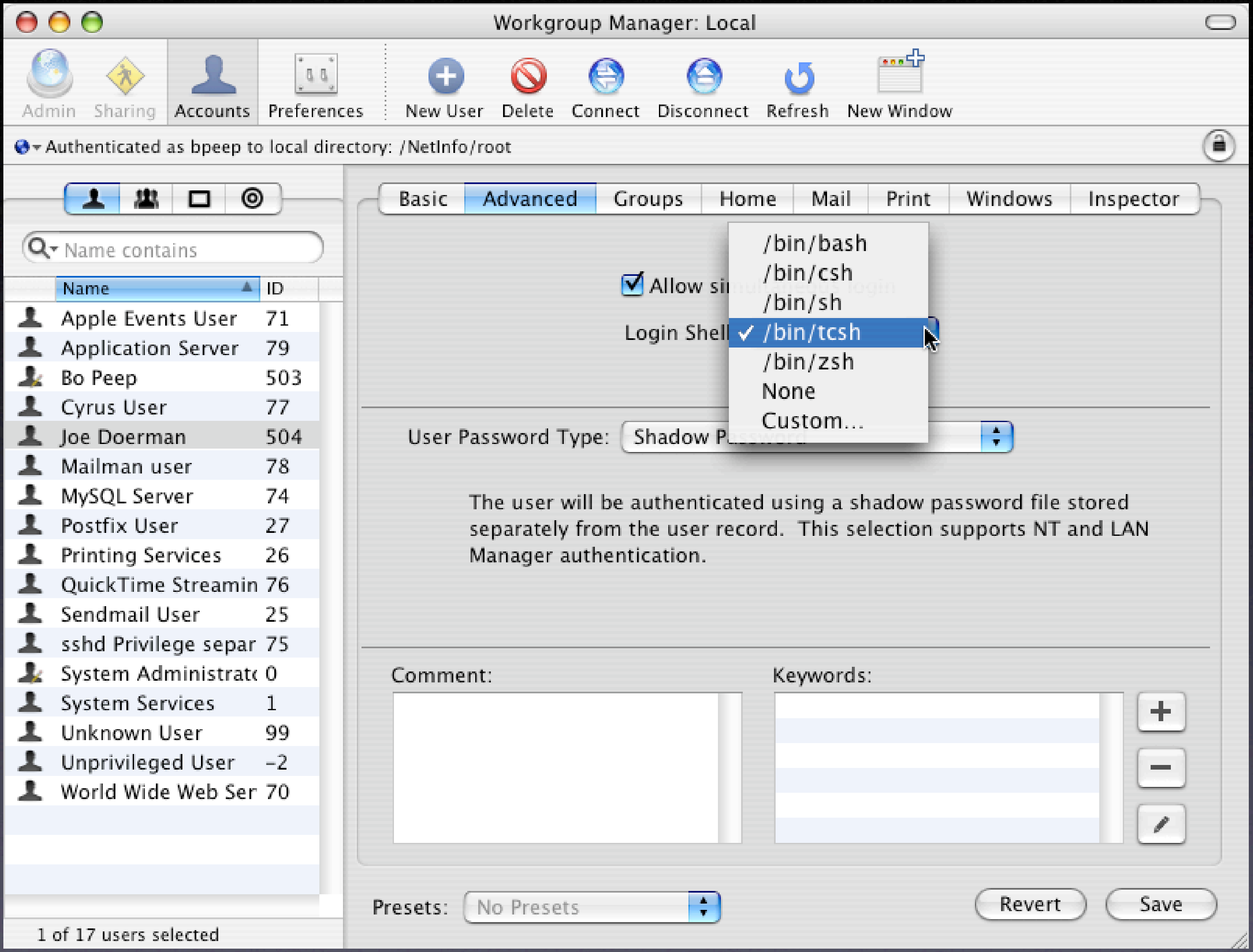
○ Execute the default login shell using /usr/bin/login

● Execute this command (specify complete path):

/bin/tcsh

Declare terminal type ($TERM) as: vt100

□ Open a saved .term file when Terminal starts:



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

☑ Allow si

Login Shell ✓ /bin/tcsh

User Password Type: Shadow Password

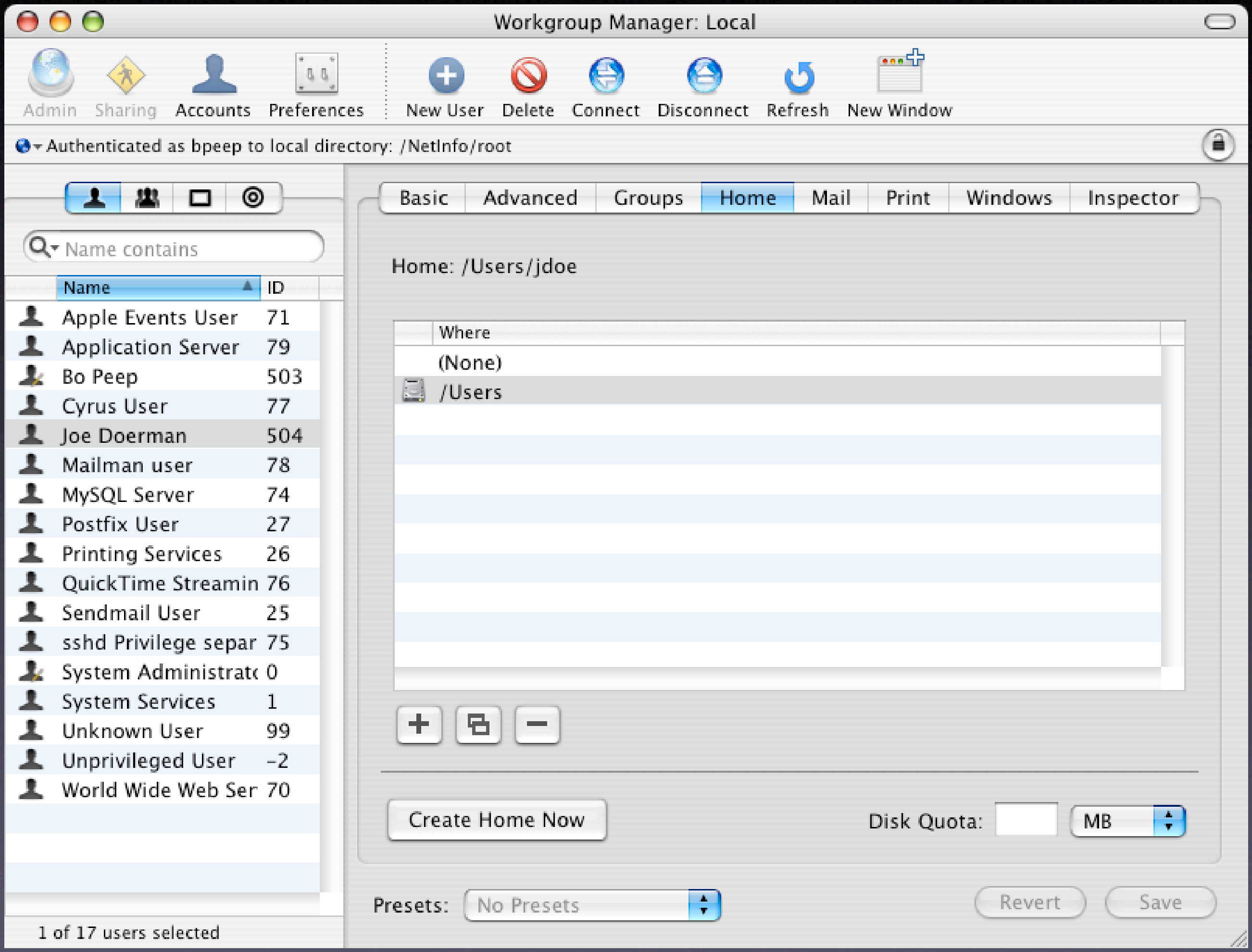
The user will be authenticated using a shadow password file stored separately from the user record. This selection supports NT and LAN Manager authentication.

Presets: No Presets

There's another place like home

- Click ruby slippers three times, and...
- Set user home directory to something other than default -- must be one or the other

The Current Home



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administrat	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

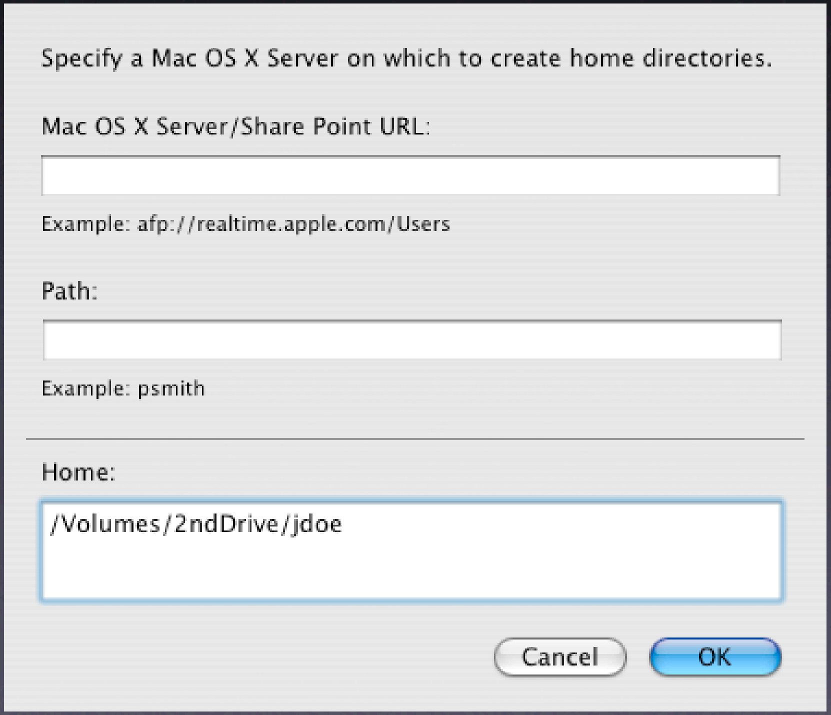
Home: /Users/jdoe

Where
(None)
/Users

Disk Quota: MB

Presets: No Presets

Setting the Home Directory



Specify a Mac OS X Server on which to create home directories.

Mac OS X Server/Share Point URL:

Example: afp://realtime.apple.com/Users

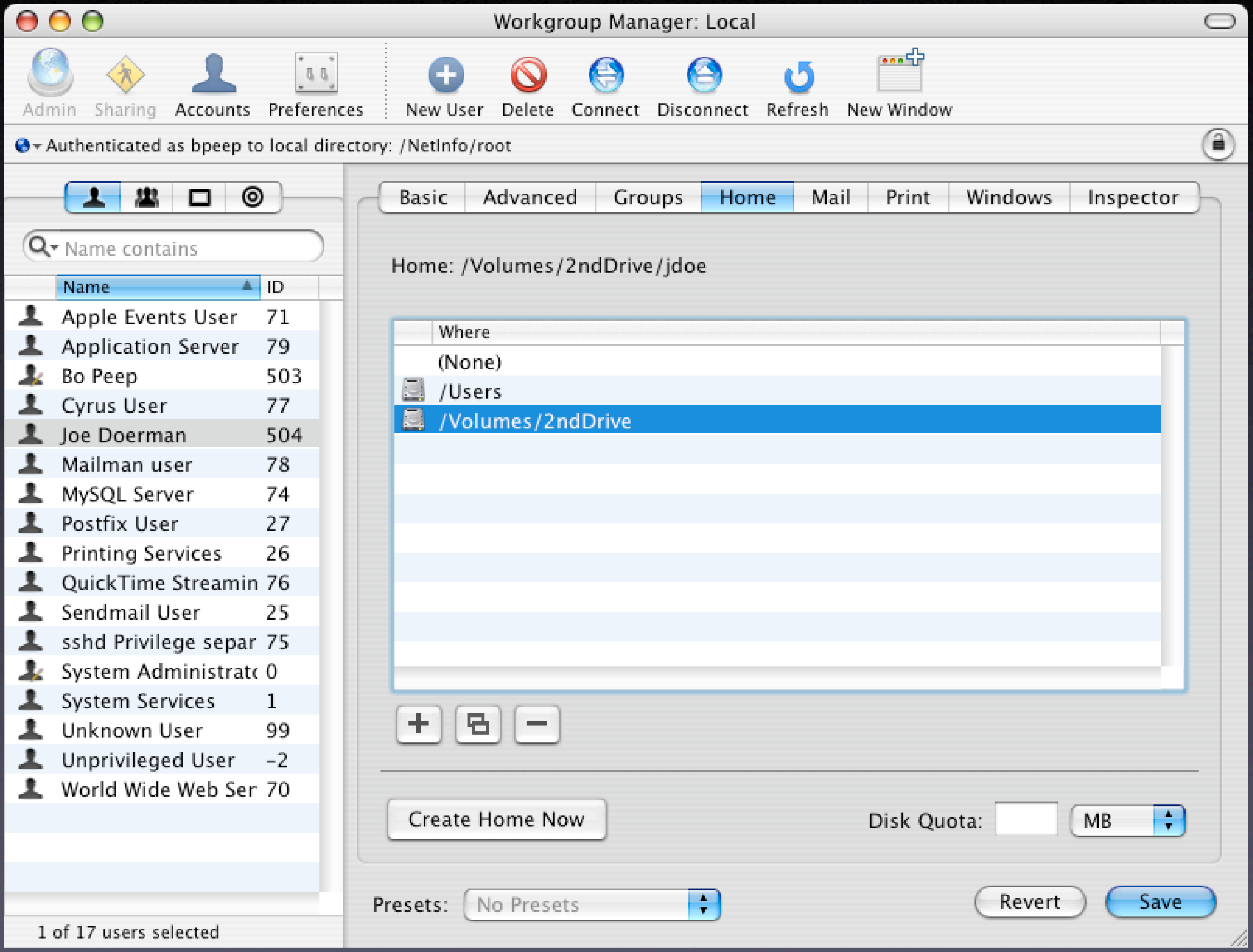
Path:

Example: psmith

Home:

/Volumes/2ndDrive/jdoe

Your New Home



Authenticated as bpeep to local directory: /NetInfo/root

Name	ID
Apple Events User	71
Application Server	79
Bo Peep	503
Cyrus User	77
Joe Doerman	504
Mailman user	78
MySQL Server	74
Postfix User	27
Printing Services	26
QuickTime Streamin	76
Sendmail User	25
sshd Privilege separ	75
System Administratc	0
System Services	1
Unknown User	99
Unprivileged User	-2
World Wide Web Ser	70

1 of 17 users selected

Home: /Volumes/2ndDrive/jdoe

Where
(None)
/Users
/Volumes/2ndDrive

Disk Quota: MB

Presets: No Presets

Application Limitations

Disallow the following:

- Installer.app
- Burn optical disks
- Disk Utility.app
- Terminal.app
- Use external media

Kiosk

- Allow only one application: Safari for a web browser station or Mail.app for a mail station

Take-away Points

Accounts

- Check your password strength with Keychain Manager info button
- Set that Master Password!
- Accounts can be managed on remote servers or locally
- Local accounts have many hidden but manageable attributes

NetInfoDatabase

- Holds all information about everything
- BACK IT UP!

NetInfo Manager

The only tool that can:

- Enable/disable root login
- Dig deeper into the NetInfo Database

System Preferences Accounts Pane

- Offers a fair amount of control over user accounts
- Is “ready to go” on your machines right now
- Is the simplest way to modify MCX settings

Workgroup Manager

- Can do almost everything NetInfo Manager can, but with a nice GUI
- Manage "hidden" user account attributes without running a server
- Offers a greater degree of control over MCX settings than System Preferences

UNIX commands for account manipulation

- `users` and `groups`
- `id`
- `dscl`
- `nicl`
- `nidump` and `niload`
- `passwd`
- `dsenableroot`

Synopsis

- What are accounts, where they live, and their care and feeding
- When to use NetInfo Manager
- Using System Preferences for accounts
- Going to town with Workgroup Manager
- Some command line goodies

Resources

- Server Admin software, including Workgroup Manager: http://www.apple.com/downloads/macosx/apple/macosxserveradmintools.html
- Workgroup Manager Technology Brief http://images.apple.com/server/pdfs/L31753A_Workgroup_TB_final.pdf
- Mac OS X: Account Capabilities - How to Allow Use of Unbundled Applications http://docs.info.apple.com/article.html?artnum=107672

Thank You!

Mac OS X Accounts

Session M235

Macworld San Francisco 2005

John Stewart & Dave Pugh

University of Michigan

Apple Certified System Administrators 10.3