

Managing FileVault 2 with fdesetup on OS X Mountain Lion

Rich Trouton

Howard Hughes Medical Institute, Janelia Farm
Research Campus
Lead Help Desk Technician

FileVault 2 Under The Hood

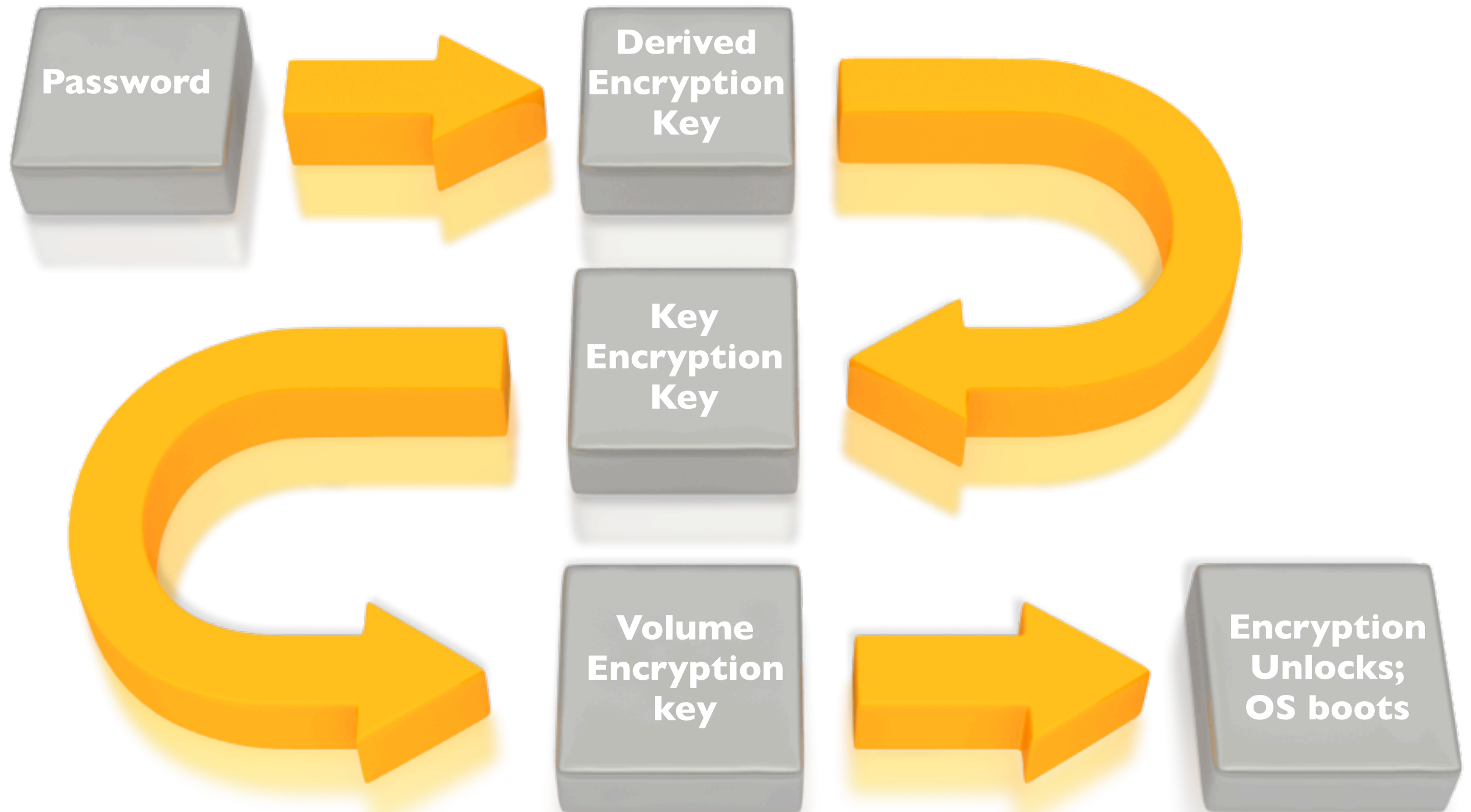


Keys Used By FileVault 2



- › Derived Encryption Key
- › Key Encryption Key
- › Volume Encryption Key

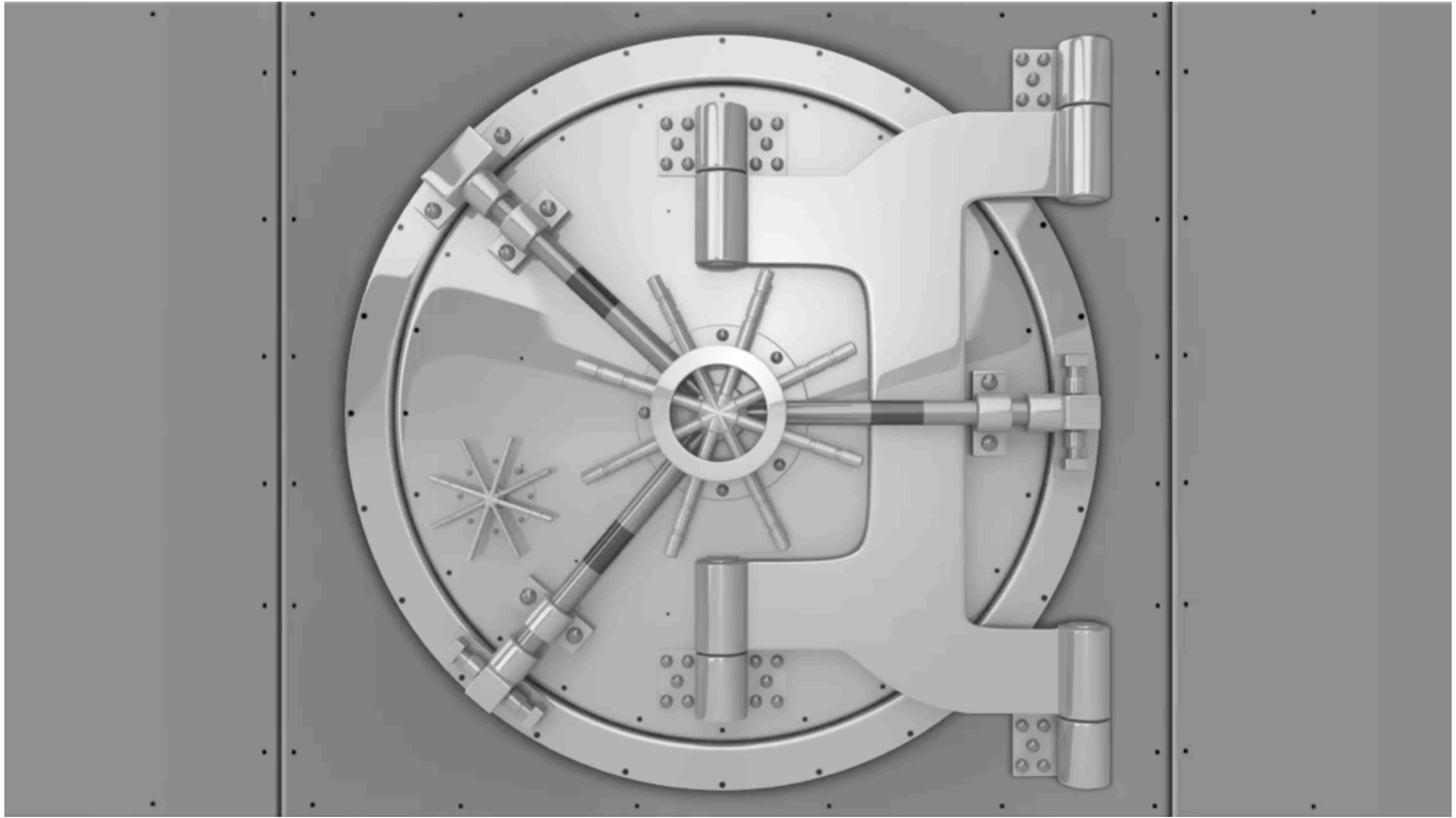
Key-Driven Unlock Process



Generating derived key from the user's password



Key validation and volume unlock



Pre-encryption access



Post-encryption access



Post-encryption access



No key? No access.



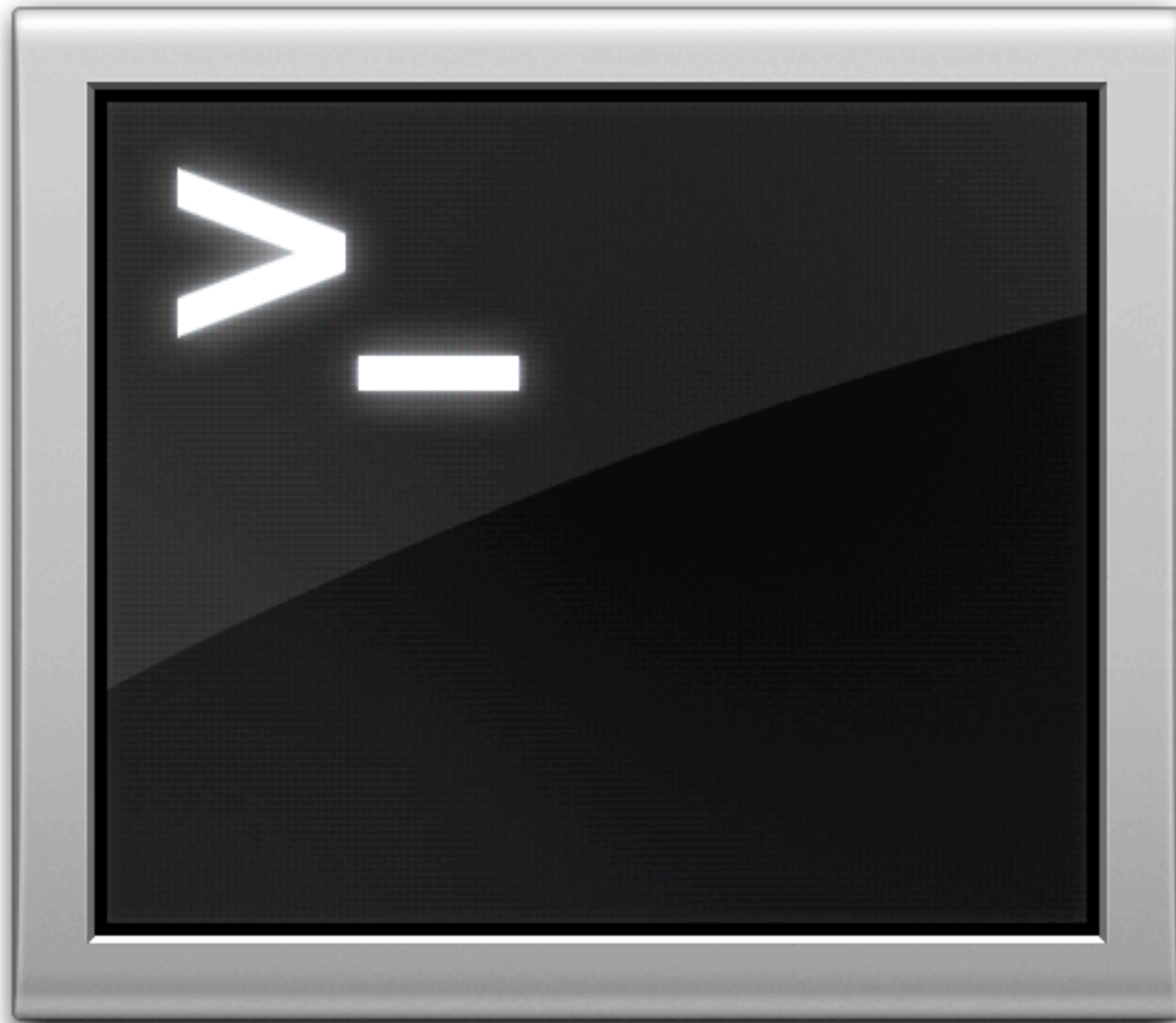
Mountain Lion's fdsetup



fdsetup overview

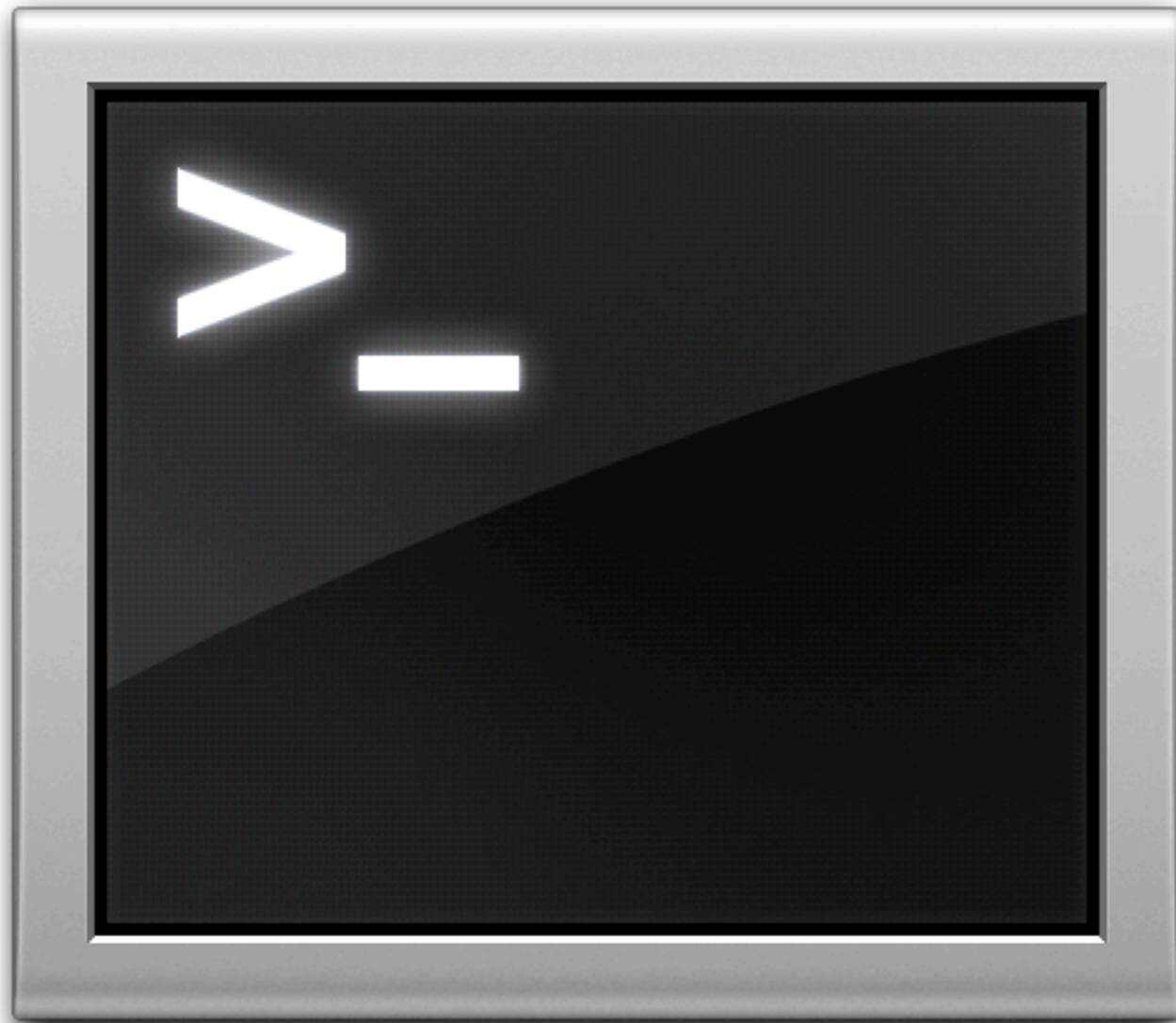


fdsetup commands



- › fdsetup enable
- › fdsetup disable
- › fdsetup add
- › fdsetup list
- › fdsetup remove
- › fdsetup sync

fdsetup enable

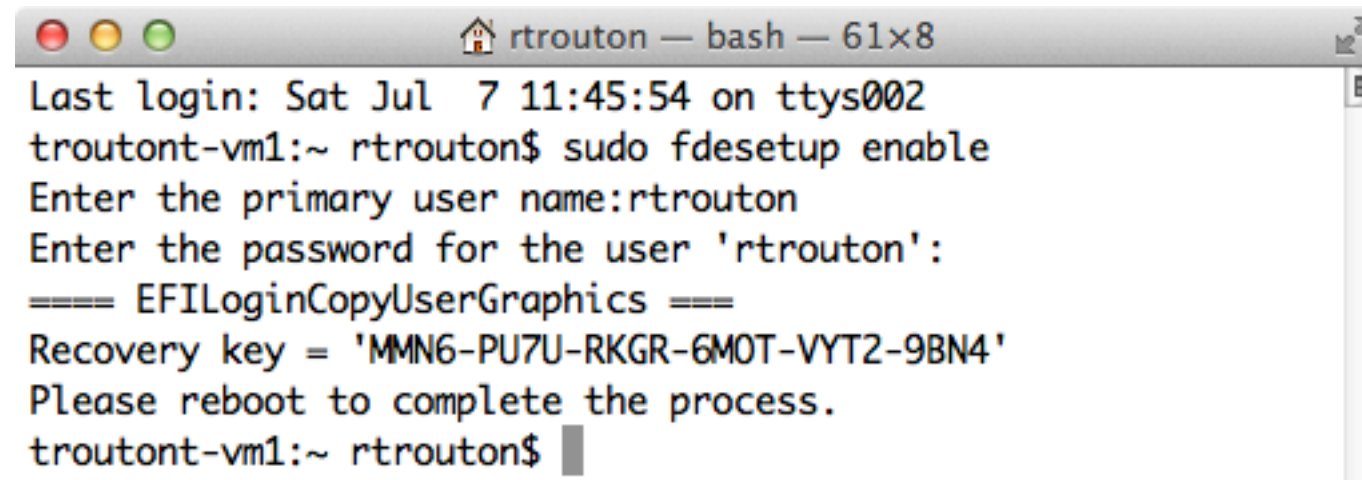


» Activates FileVault 2 Encryption

- Can set FileVault 2 encryption to use:
 - Individual alphanumeric recovery key
 - Institutional recovery key using FileVaultMaster.keychain
 - Both kinds of recovery key simultaneously
- Can enable multiple user accounts at time of encryption activation
- Can import user and certificate information

fdsetup enable

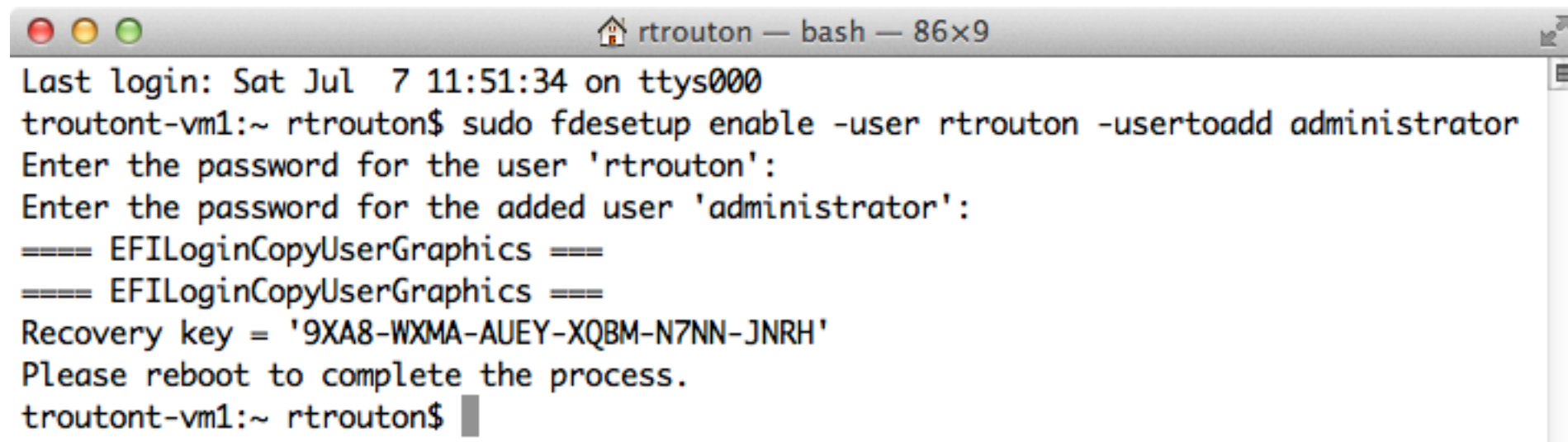
sudo fdsetup enable

A terminal window with a title bar showing 'rtrouton — bash — 61x8'. The terminal output shows the command 'sudo fdsetup enable' being executed. It prompts for the primary user name 'rtrouton' and the password. After successful execution, it displays the recovery key 'MMN6-PU7U-RKGR-6MOT-VYT2-9BN4' and instructs the user to reboot. The prompt returns to 'troutont-vm1:~ rtrouton\$'.

```
troutont-vm1:~ rtrouton$ sudo fdsetup enable
Last login: Sat Jul  7 11:45:54 on ttys002
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
==== EFILoginCopyUserGraphics ====
Recovery key = 'MMN6-PU7U-RKGR-6MOT-VYT2-9BN4'
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

fdsetup enable -user

sudo fdsetup enable -user username -usertoadd username

A terminal window titled 'rtrouton — bash — 86x9' with standard macOS window controls. The terminal output shows the execution of 'sudo fdsetup enable -user rtrouton -usertoadd administrator'. It prompts for the password for 'rtrouton' and then for the added user 'administrator'. After successful execution, it displays the recovery key '9XA8-WXMA-AUEY-XQBM-N7NN-JNRH' and instructs the user to reboot. The prompt returns to 'troutont-vm1:~ rtrouton\$'.

```
troutont-vm1:~ rtrouton$ sudo fdsetup enable -user rtrouton -usertoadd administrator
Enter the password for the user 'rtrouton':
Enter the password for the added user 'administrator':
==== EFILoginCopyUserGraphics ====
==== EFILoginCopyUserGraphics ====
Recovery key = '9XA8-WXMA-AUEY-XQBM-N7NN-JNRH'
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

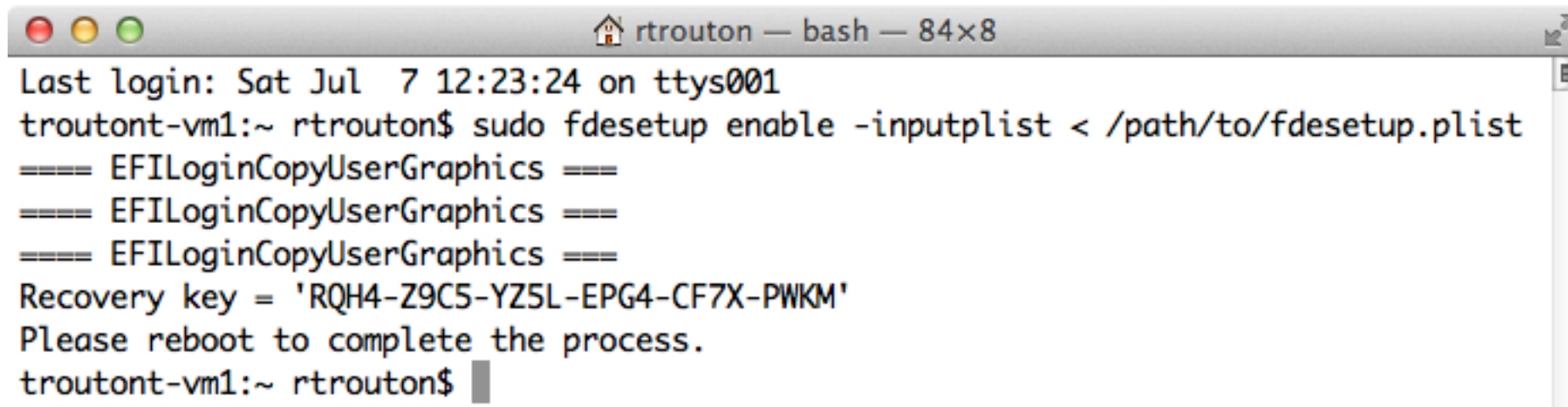
fdsetup enable -inputplist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Username</key>
    <string>localadmin</string>
    <key>Password</key>
    <string>password</string>
    <key>AdditionalUsers</key>
    <array>
      <dict>
        <key>Username</key>
        <string>tom</string>
        <key>Password</key>
        <string>password</string>
      </dict>
      <dict>
        <key>Username</key>
        <string>harry</string>
        <key>Password</key>
        <string>password</string>
      </dict>
    </array>
  </dict>
</plist>
```

Note: All account passwords need to be supplied in cleartext.

fdsetup enable -inputplist

sudo fdsetup enable -inputplist < plistfile.plist

A terminal window titled 'rtrouton — bash — 84x8' with standard macOS window controls (red, yellow, green buttons). The terminal shows the output of the 'fdsetup' command. It starts with a login message, followed by the command 'sudo fdsetup enable -inputplist < /path/to/fdsetup.plist'. The output consists of three lines of '==== EFILoginCopyUserGraphics ===', a recovery key, and a reboot instruction. The prompt returns to the user.

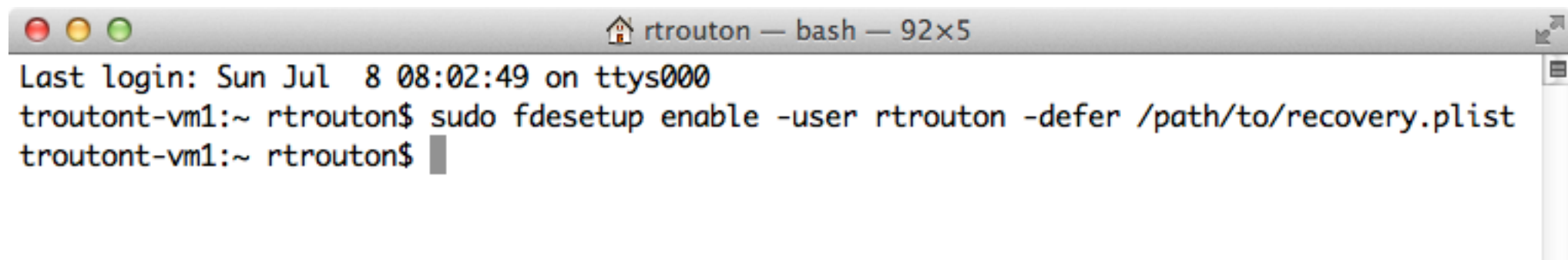
```
rtrouton — bash — 84x8
Last login: Sat Jul  7 12:23:24 on ttys001
troutont-vm1:~ rtrouton$ sudo fdsetup enable -inputplist < /path/to/fdsetup.plist
==== EFILoginCopyUserGraphics ===
==== EFILoginCopyUserGraphics ===
==== EFILoginCopyUserGraphics ===
Recovery key = 'RQH4-Z9C5-YZ5L-EPG4-CF7X-PWKM'
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

fdsetup enable -defer

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>EnabledDate</key>
  <string>2012-07-08 08:05:54 -0400</string>
  <key>HardwareUUID</key>
  <string>00000000-0000-1000-8000-000C293DEFEC</string>
  <key>LVGUID</key>
  <string>B7990442-91D1-4F5E-8F04-DDAC7B3610F2</string>
  <key>LVUUID</key>
  <string>FF837400-B781-496E-8992-D5A11B5A1139</string>
  <key>PVUUID</key>
  <string>E0FD9F00-5D41-4597-A10B-73F0A463CC65</string>
  <key>RecoveryKey</key>
  <string>8MGZ-C7BL-ML2M-J6B4-HN35-ZDOA</string>
  <key>SerialNumber</key>
  <string>VMWVk2fm2om0q0/em3zWsLr2g</string>
</dict>
</plist>
```

`fdsetup enable -defer`

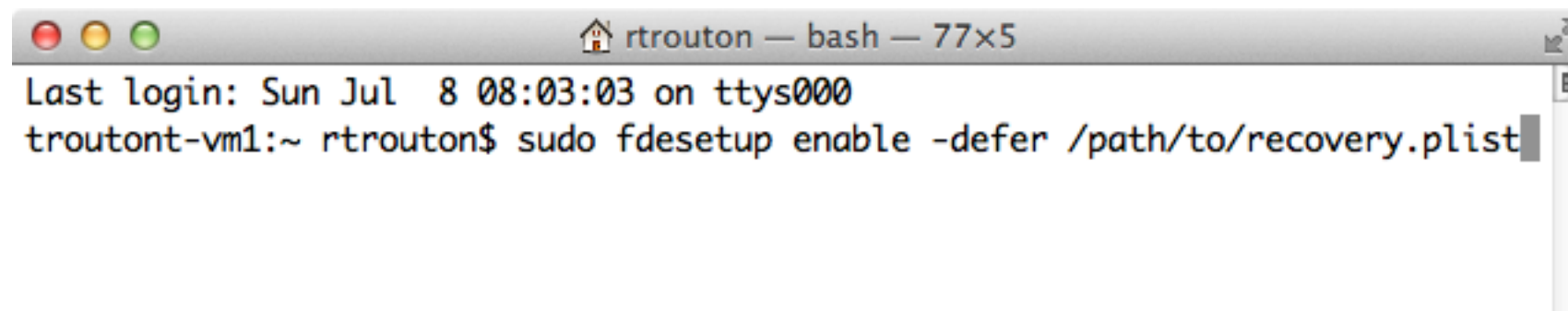
`sudo fdsetup enable -user username -defer plistfile.plist`

A screenshot of a macOS-style terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left, a home icon followed by the text "rtrouton — bash — 92x5" in the center, and a close button on the right. The terminal content shows a login message "Last login: Sun Jul 8 08:02:49 on ttys000", followed by a prompt "troutont-vm1:~ rtrouton\$". The user has entered the command "sudo fdsetup enable -user rtrouton -defer /path/to/recovery.plist", and the prompt "troutont-vm1:~ rtrouton\$" is shown again with a cursor at the end. A vertical scrollbar is visible on the right side of the terminal window.

```
Last login: Sun Jul 8 08:02:49 on ttys000
troutont-vm1:~ rtrouton$ sudo fdsetup enable -user rtrouton -defer /path/to/recovery.plist
troutont-vm1:~ rtrouton$
```

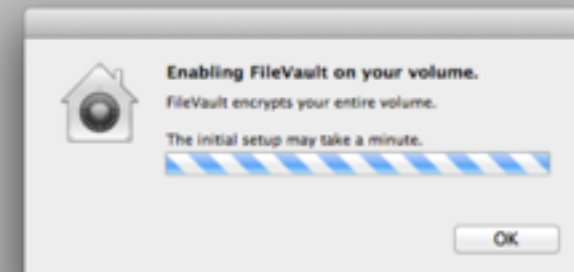
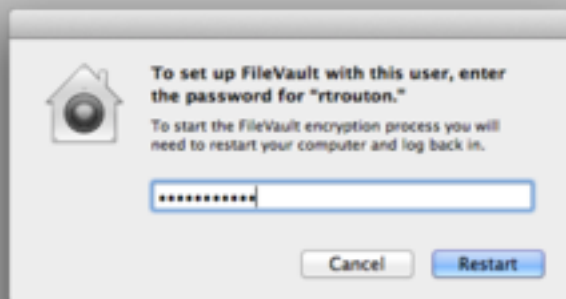
fdsetup enable -defer

sudo fdsetup enable -defer plistfile.plist

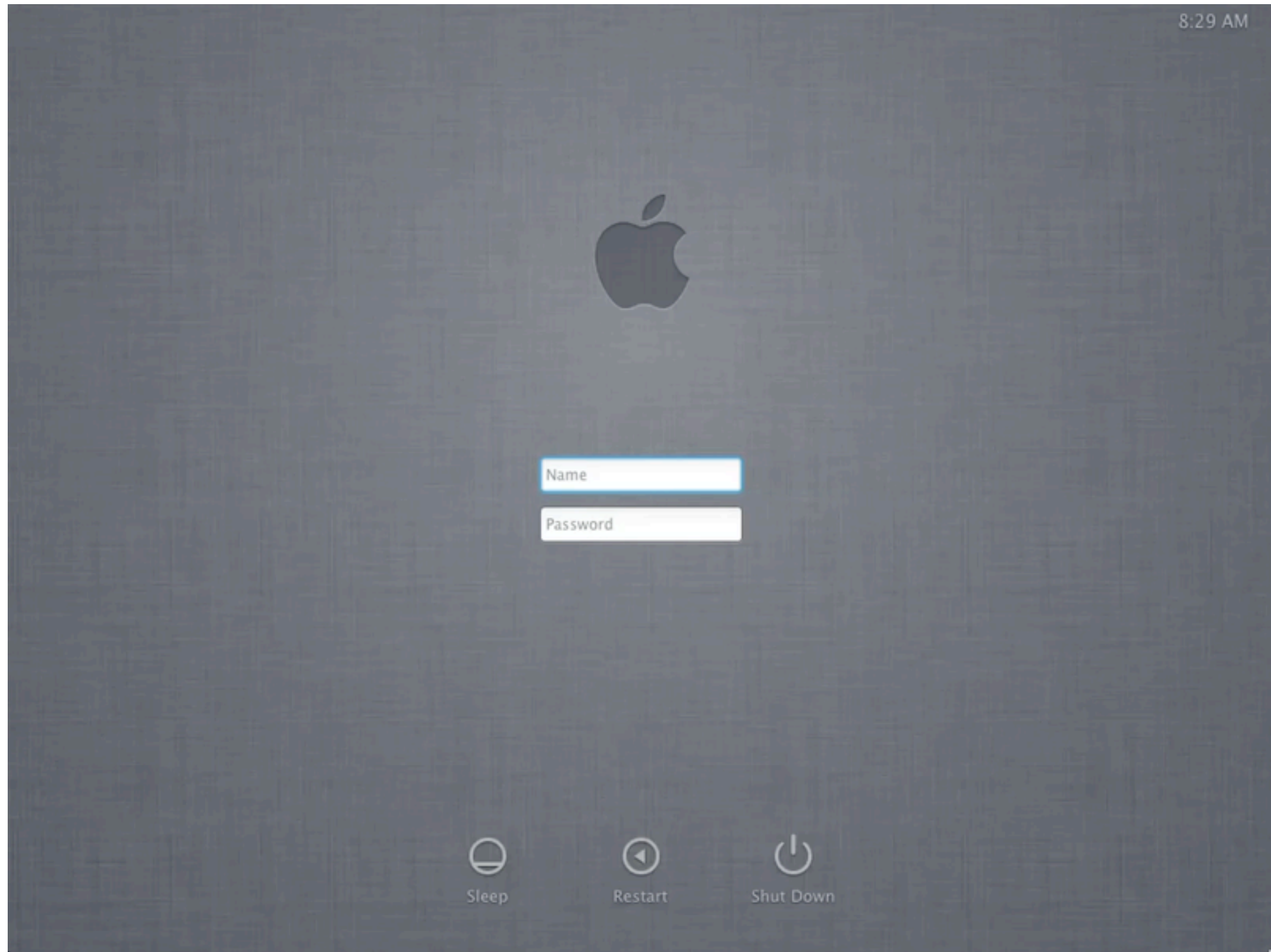
A screenshot of a macOS terminal window. The title bar shows a home icon, the text 'rtrouton — bash — 77x5', and window control buttons. The terminal content shows a login message and a command being executed.

```
Last login: Sun Jul  8 08:03:03 on ttys000
troutont-vm1:~ rtrouton$ sudo fdsetup enable -defer /path/to/recovery.plist
```


fdsetup enable -defer

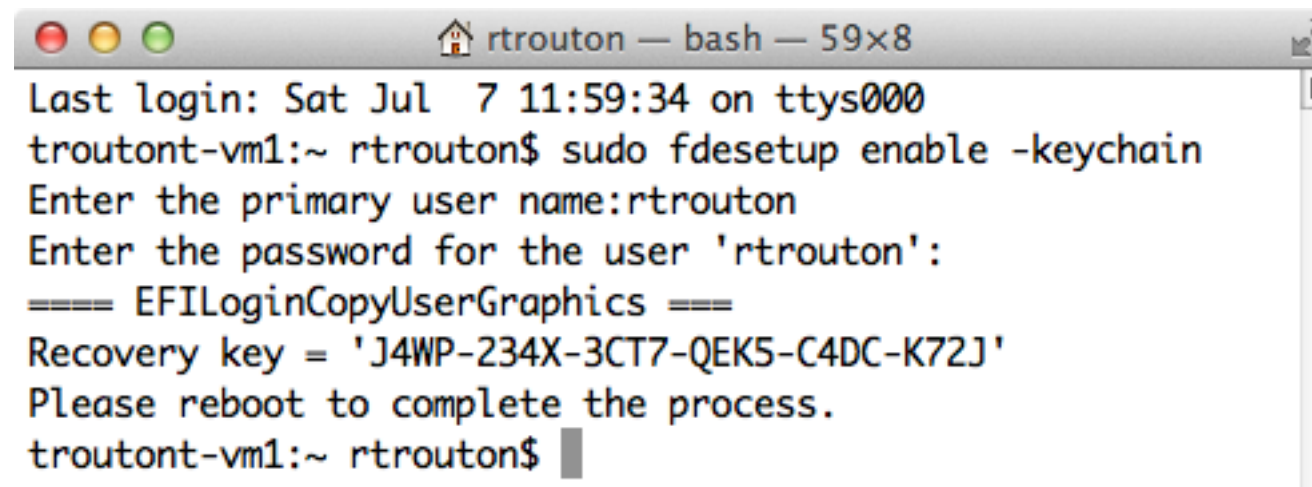


fdsetup enable -defer



fdsetup enable -keychain

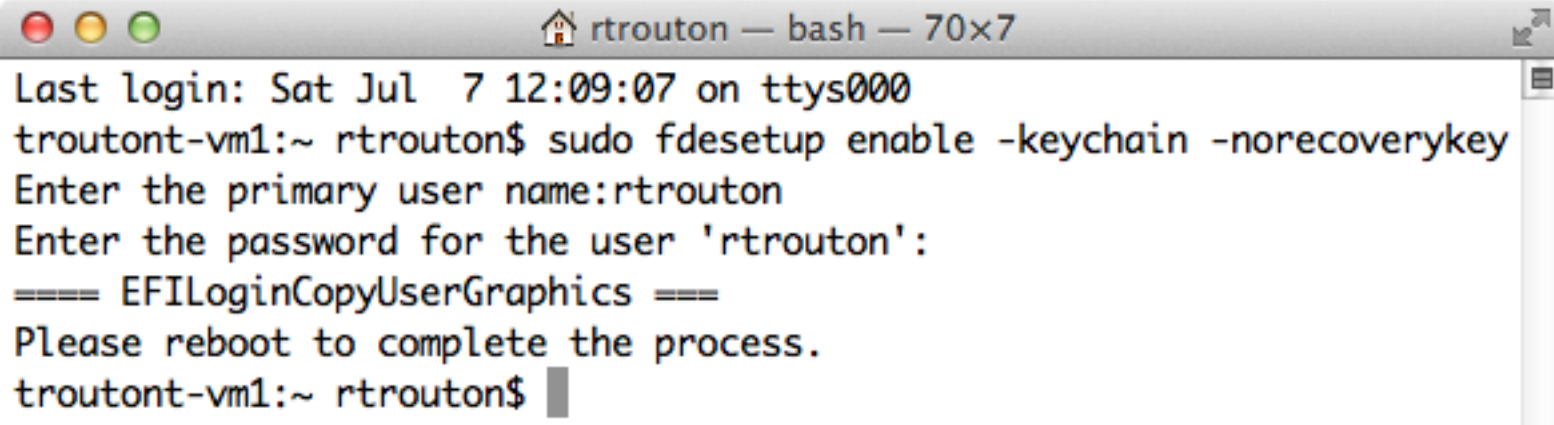
sudo fdsetup enable -keychain

A terminal window titled 'rtrouton — bash — 59x8' with standard macOS window controls. The terminal output shows the execution of 'sudo fdsetup enable -keychain'. It prompts for the primary user name (rtrouton) and password. It then displays the recovery key 'J4WP-234X-3CT7-QEK5-C4DC-K72J' and instructs the user to reboot to complete the process. The prompt returns to 'troutont-vm1:~ rtrouton\$'.

```
troutont-vm1:~ rtrouton$ sudo fdsetup enable -keychain
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
==== EFILoginCopyUserGraphics ====
Recovery key = 'J4WP-234X-3CT7-QEK5-C4DC-K72J'
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

fdsetup enable -keychain

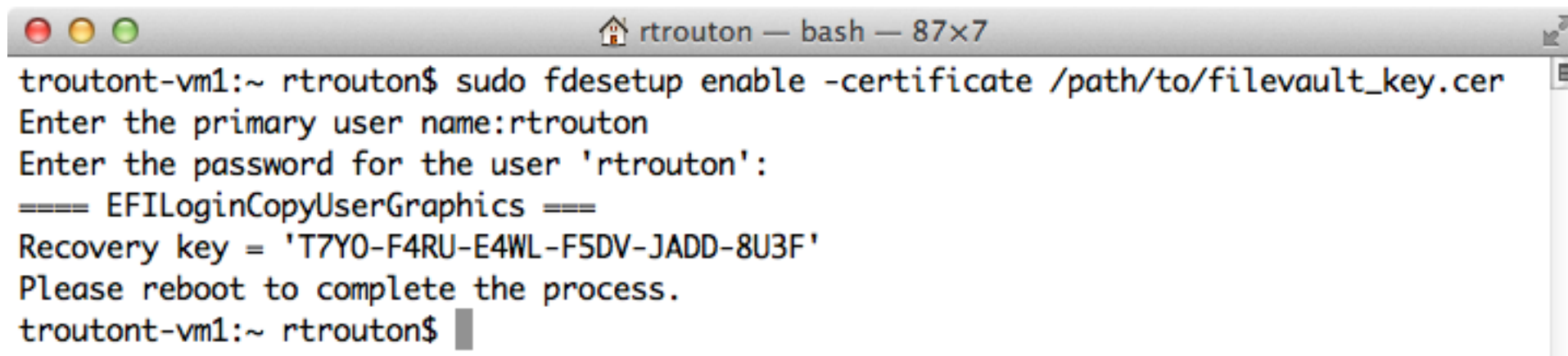
sudo fdsetup enable -keychain -norecoverykey

A terminal window titled "rtrouton — bash — 70x7" with standard macOS window controls (red, yellow, green buttons). The terminal output shows the user logging in, running the command "sudo fdsetup enable -keychain -norecoverykey", and receiving instructions to enter the primary user name and password. The output concludes with "==== EFILoginCopyUserGraphics ====" and "Please reboot to complete the process." followed by a new command prompt.

```
rtrouton — bash — 70x7
Last login: Sat Jul  7 12:09:07 on ttys000
troutont-vm1:~ rtrouton$ sudo fdsetup enable -keychain -norecoverykey
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
==== EFILoginCopyUserGraphics ====
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```


fdsetup enable -certificate

sudo fdsetup enable -certificate cert.cer

A terminal window with a title bar showing 'rtrouton — bash — 87x7'. The terminal text is as follows:

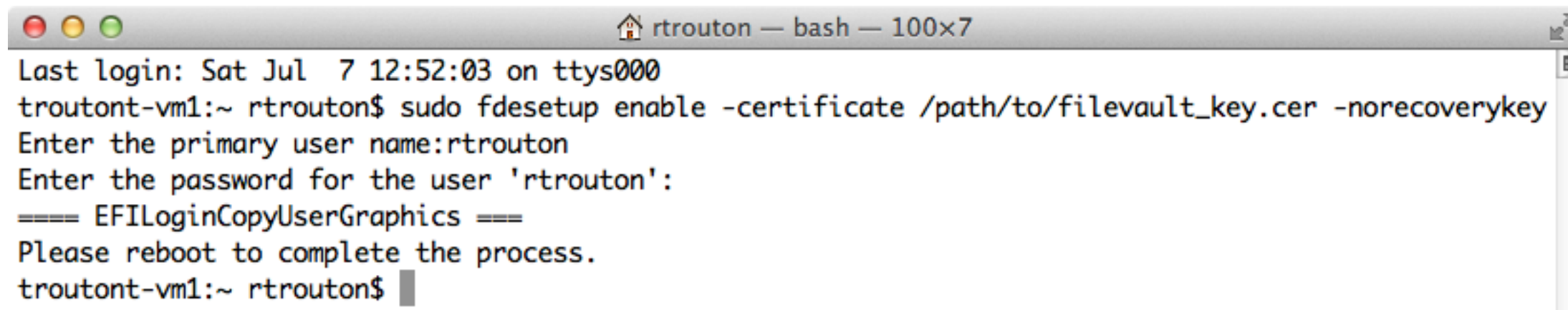
```
troutont-vm1:~ rtrouton$ sudo fdsetup enable -certificate /path/to/filevault_key.cer
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
==== EFILoginCopyUserGraphics ====
Recovery key = 'T7Y0-F4RU-E4WL-F5DV-JADD-8U3F'
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

fdsetup enable -certificate



fdsetup enable -certificate

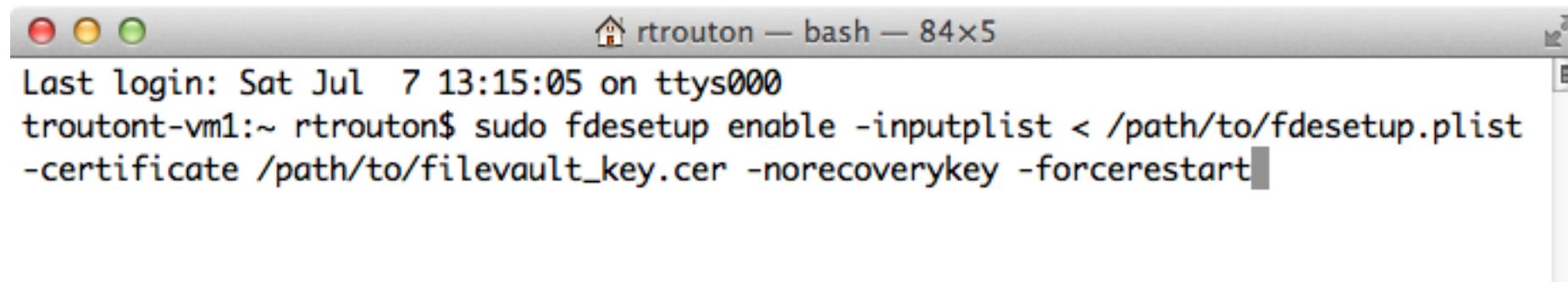
sudo fdsetup enable -certificate cert.cer -norecoverykey

A terminal window titled 'rtrouton — bash — 100x7' with standard macOS window controls (red, yellow, green buttons). The terminal output shows the user logging in, running the 'fdsetup' command with the '-certificate' and '-norecoverykey' flags, and receiving instructions to reboot. The prompt returns to the user after the command execution.

```
troutont-vm1:~ rtrouton$ sudo fdsetup enable -certificate /path/to/filevault_key.cer -norecoverykey
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
==== EFILoginCopyUserGraphics ====
Please reboot to complete the process.
troutont-vm1:~ rtrouton$
```

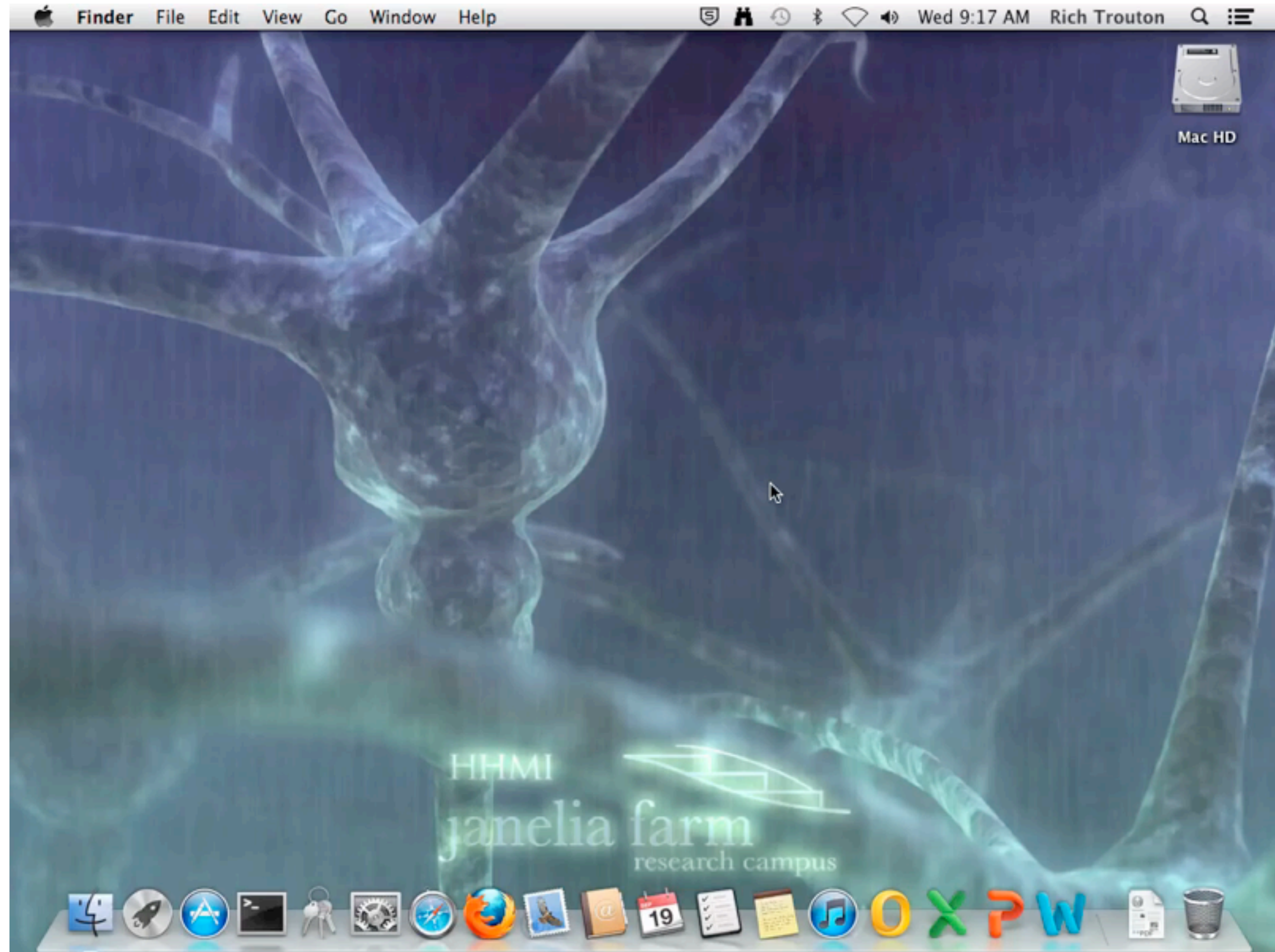
fdsetup enable -forcerestart

sudo fdsetup enable -inputplist < plistfile.plist-certificate cert.cer -norecoverykey -forcerestart

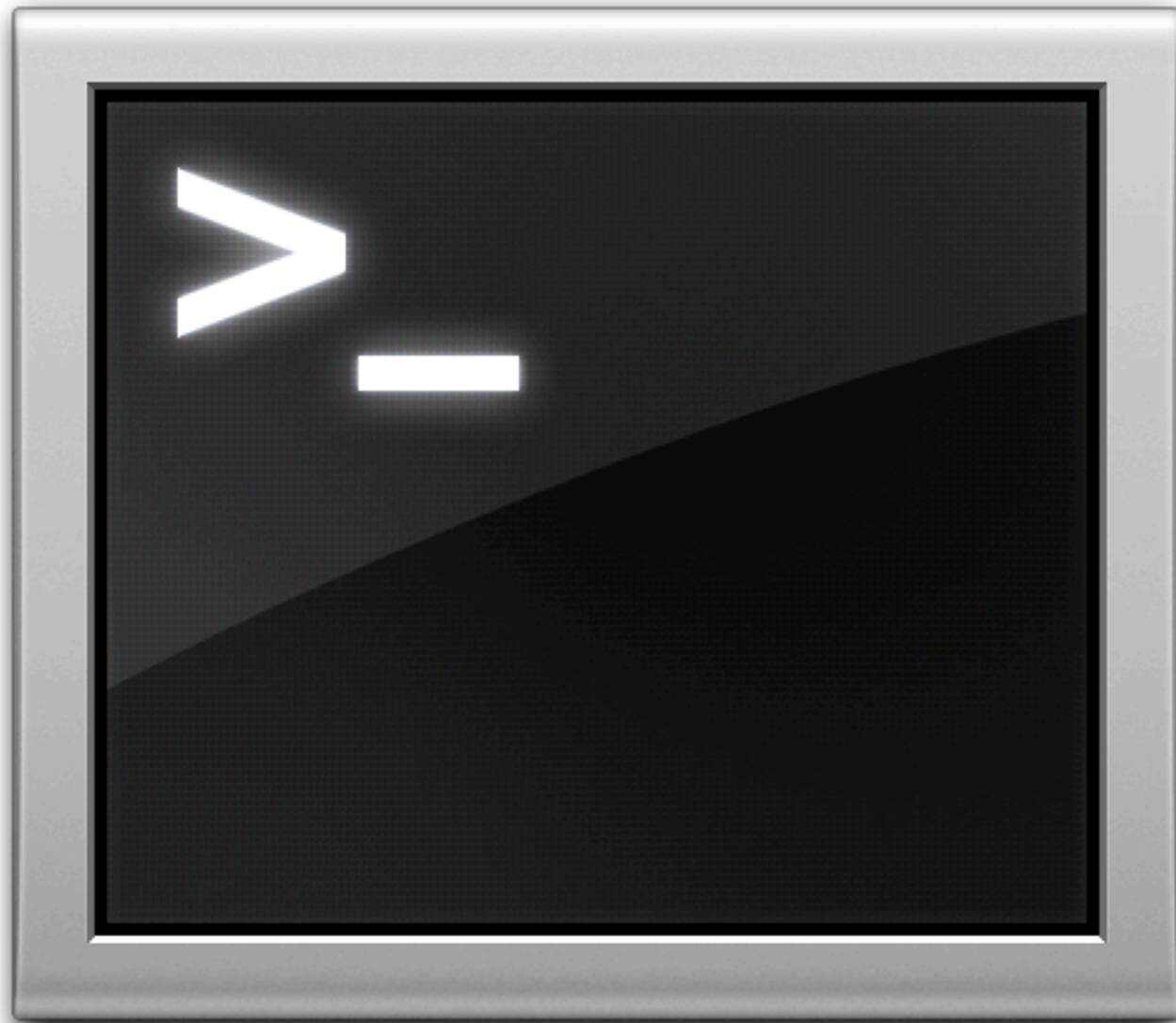
A screenshot of a macOS terminal window. The title bar shows a home icon, the text 'rtrouton — bash — 84x5', and window control buttons. The terminal content shows a login message and a command being executed with sudo. The command is 'fdsetup enable -inputplist < /path/to/fdsetup.plist -certificate /path/to/filevault_key.cer -norecoverykey -forcerestart'.

```
rtrouton — bash — 84x5
Last login: Sat Jul  7 13:15:05 on ttys000
troutont-vm1:~ rtrouton$ sudo fdsetup enable -inputplist < /path/to/fdsetup.plist
-norecoverykey -forcerestart
```


fdsetup enable --forcerestart

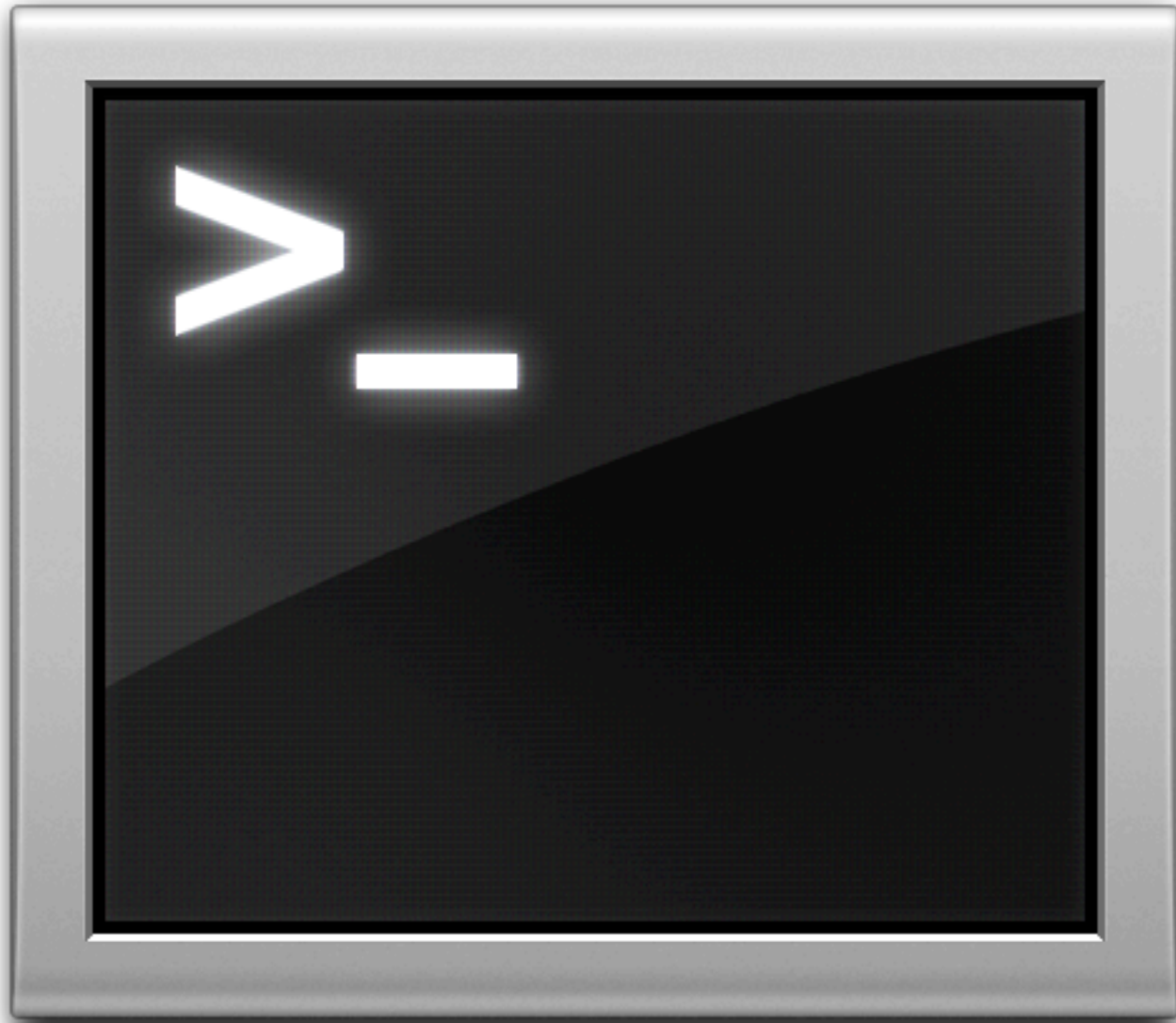


fdsetup disable



› Disables FileVault 2 encryption

fdsetup add

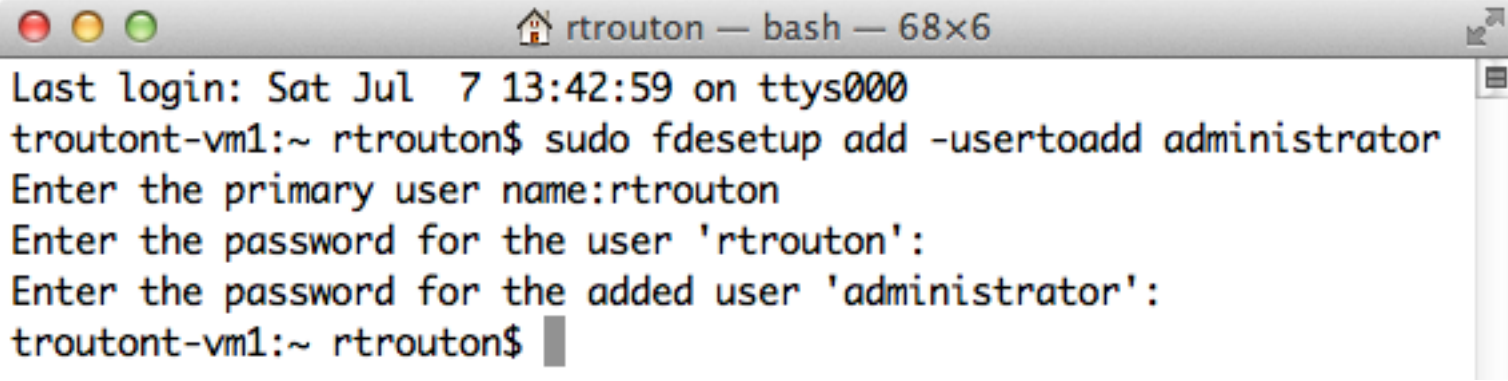


› Enables additional accounts after FileVault 2 encryption is complete

- Can enable multiple user accounts
- Can import user information

fdsetup add -usertoadd

sudo fdsetup add -usertoadd username



```
trouton — bash — 68x6
Last login: Sat Jul  7 13:42:59 on ttys000
troutont-vm1:~ rtrouton$ sudo fdsetup add -usertoadd administrator
Enter the primary user name:rtrouton
Enter the password for the user 'rtrouton':
Enter the password for the added user 'administrator':
troutont-vm1:~ rtrouton$
```

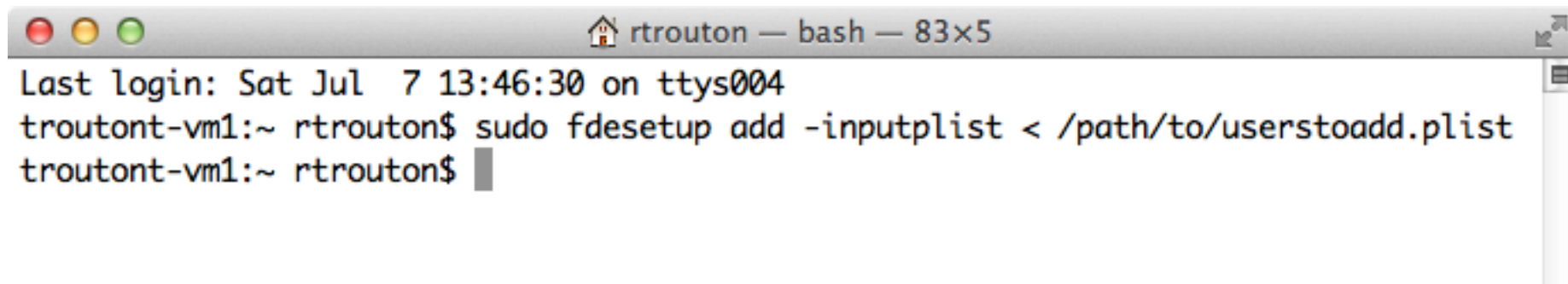
fdsetup add -inputplist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>Username</key>
<string>rtrouton</string>
<key>Password</key>
<string>password</string>
<key>AdditionalUsers</key>
<array>
  <dict>
    <key>Username</key>
    <string>fcheeryble</string>
    <key>Password</key>
    <string>password</string>
  </dict>
  <dict>
    <key>Username</key>
    <string>nnickleby</string>
    <key>Password</key>
    <string>password</string>
  </dict>
</array>
</dict>
</plist>
```

Note: All account passwords need to be supplied in cleartext.

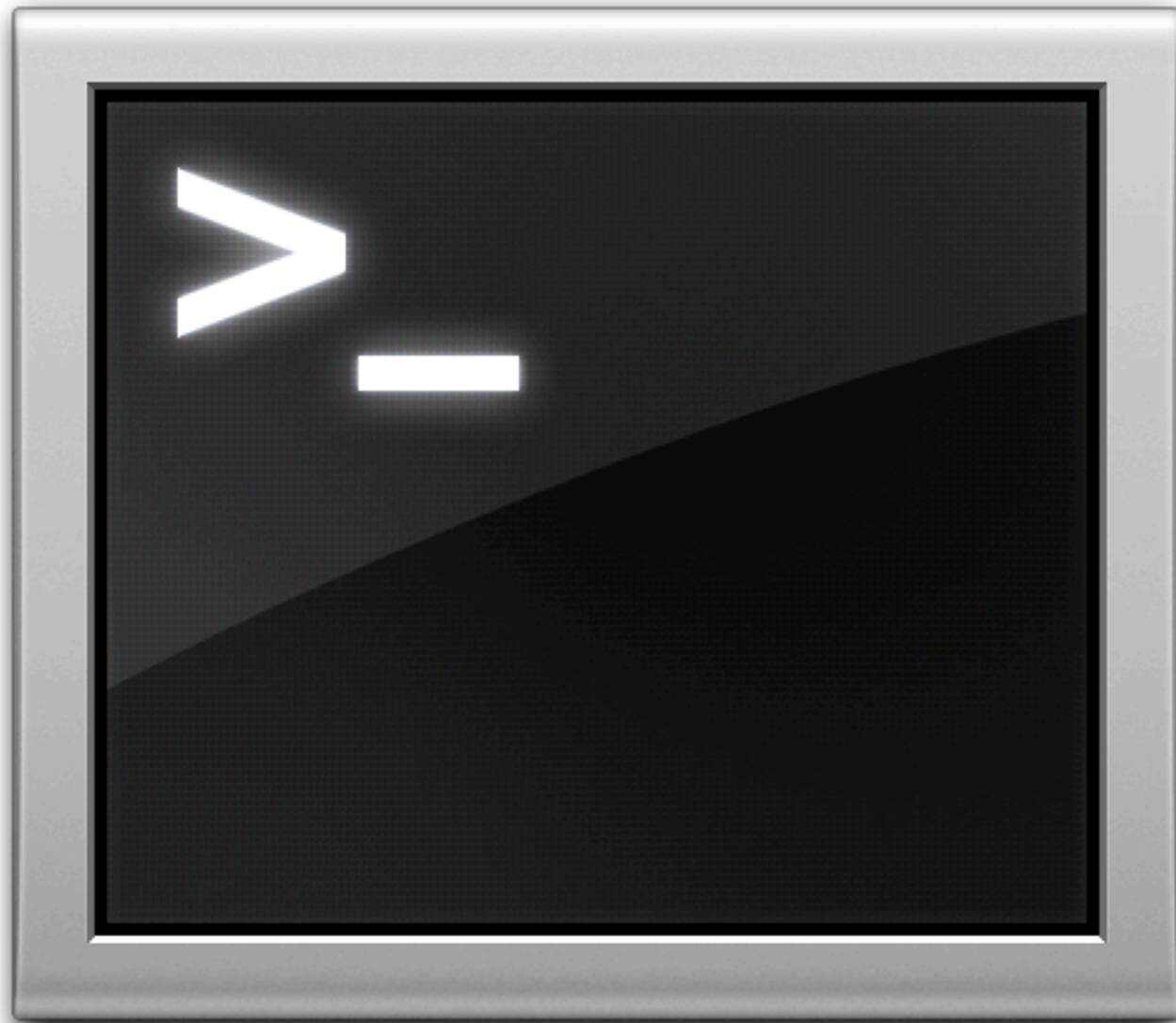
fdsetup add -inputplist

sudo fdsetup add -inputplist /path/to/plistname.plist

A screenshot of a macOS terminal window. The title bar shows a home icon, the text 'rtrouton — bash — 83x5', and window control buttons. The terminal content shows a login message, a command being executed with sudo, and the prompt returning. The command is 'fdsetup add -inputplist < /path/to/userstoadd.plist'.

```
troutont-vm1:~ rtrouton$ sudo fdsetup add -inputplist < /path/to/userstoadd.plist
troutont-vm1:~ rtrouton$
```


fdsetup list

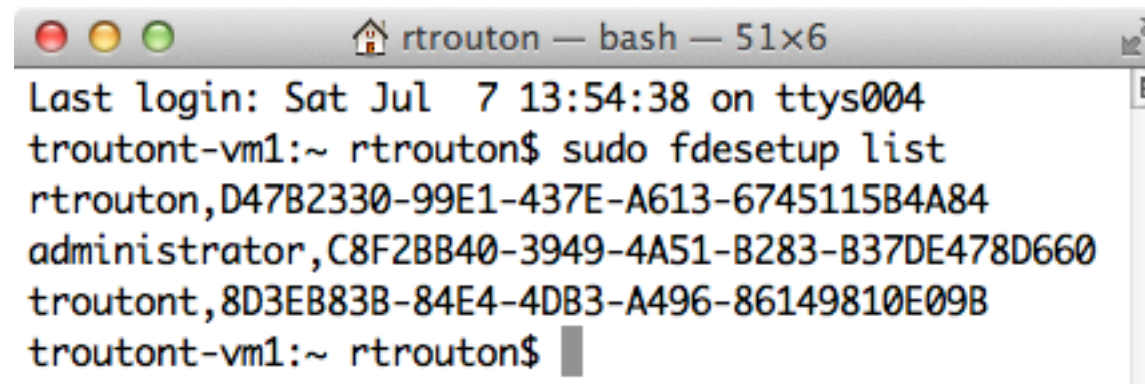


› Displays enabled accounts

- List includes the accounts' usernames and UUIDs

fdsetup list

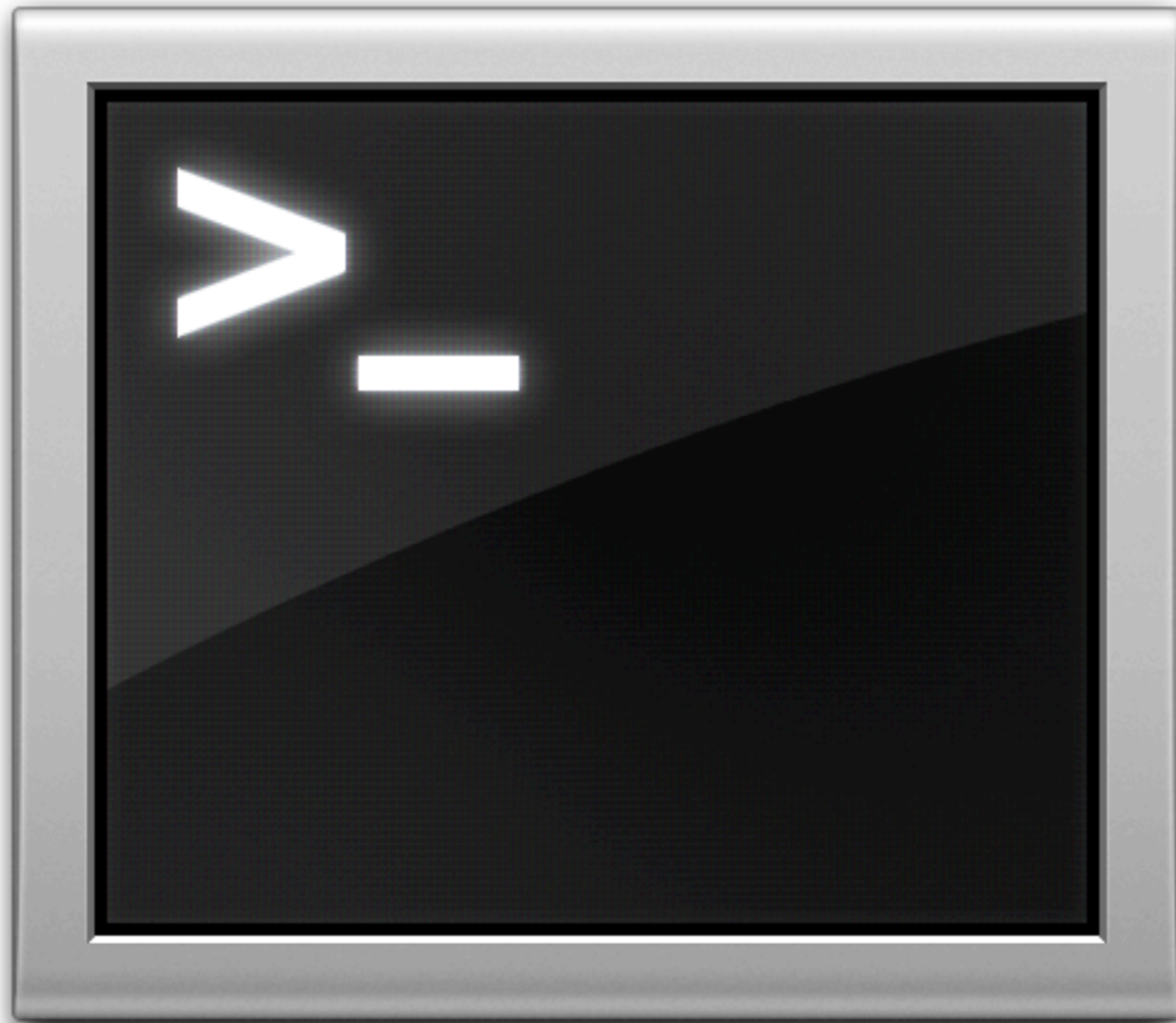
sudo fdsetup list



```
troutont-vm1:~ rtrouton$ sudo fdsetup list
rtrouton,D47B2330-99E1-437E-A613-6745115B4A84
administrator,C8F2BB40-3949-4A51-B283-B37DE478D660
troutont,8D3EB83B-84E4-4DB3-A496-86149810E09B
troutont-vm1:~ rtrouton$
```

A terminal window titled "rtrouton — bash — 51x6" showing the execution of the command "sudo fdsetup list". The output lists three entries, each consisting of a name and a UUID. The entries are: "rtrouton,D47B2330-99E1-437E-A613-6745115B4A84", "administrator,C8F2BB40-3949-4A51-B283-B37DE478D660", and "troutont,8D3EB83B-84E4-4DB3-A496-86149810E09B". The prompt "troutont-vm1:~ rtrouton\$" is shown at the end of the output.

fdsetup remove

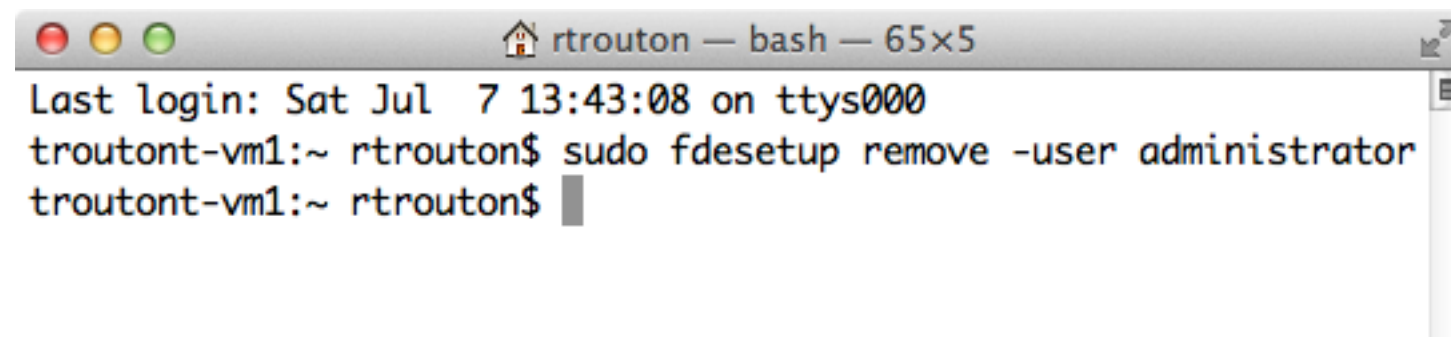


› Removes accounts from the list of FileVault 2 enabled accounts

- Can disable using account username
- Can disable using account UUID

`fdsetup remove -user`

`sudo fdsetup remove -user username`

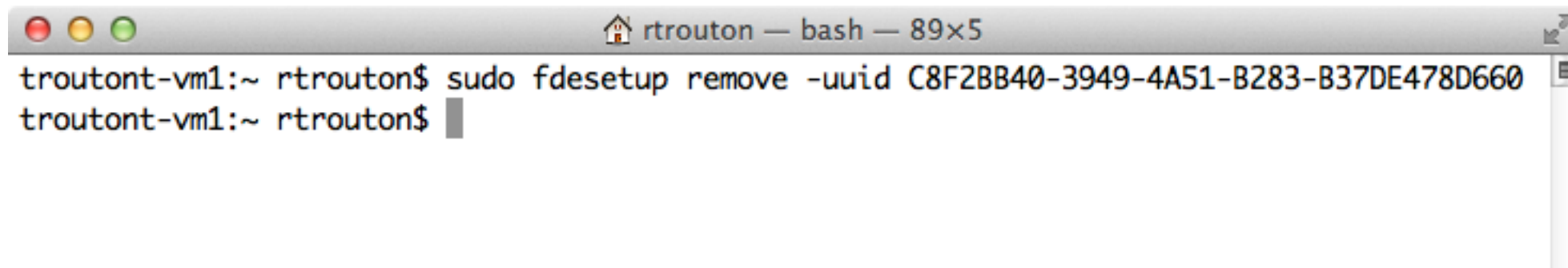


```
troutont-vm1:~ rtrouton$ sudo fdsetup remove -user administrator
```

A terminal window titled "rtrouton — bash — 65x5" with standard macOS window controls. The terminal shows the command `sudo fdsetup remove -user administrator` being executed. The prompt is `troutont-vm1:~ rtrouton$`. The output shows the last login time: `Last login: Sat Jul 7 13:43:08 on ttys000`. The command execution is successful, and the prompt returns to `troutont-vm1:~ rtrouton$`.

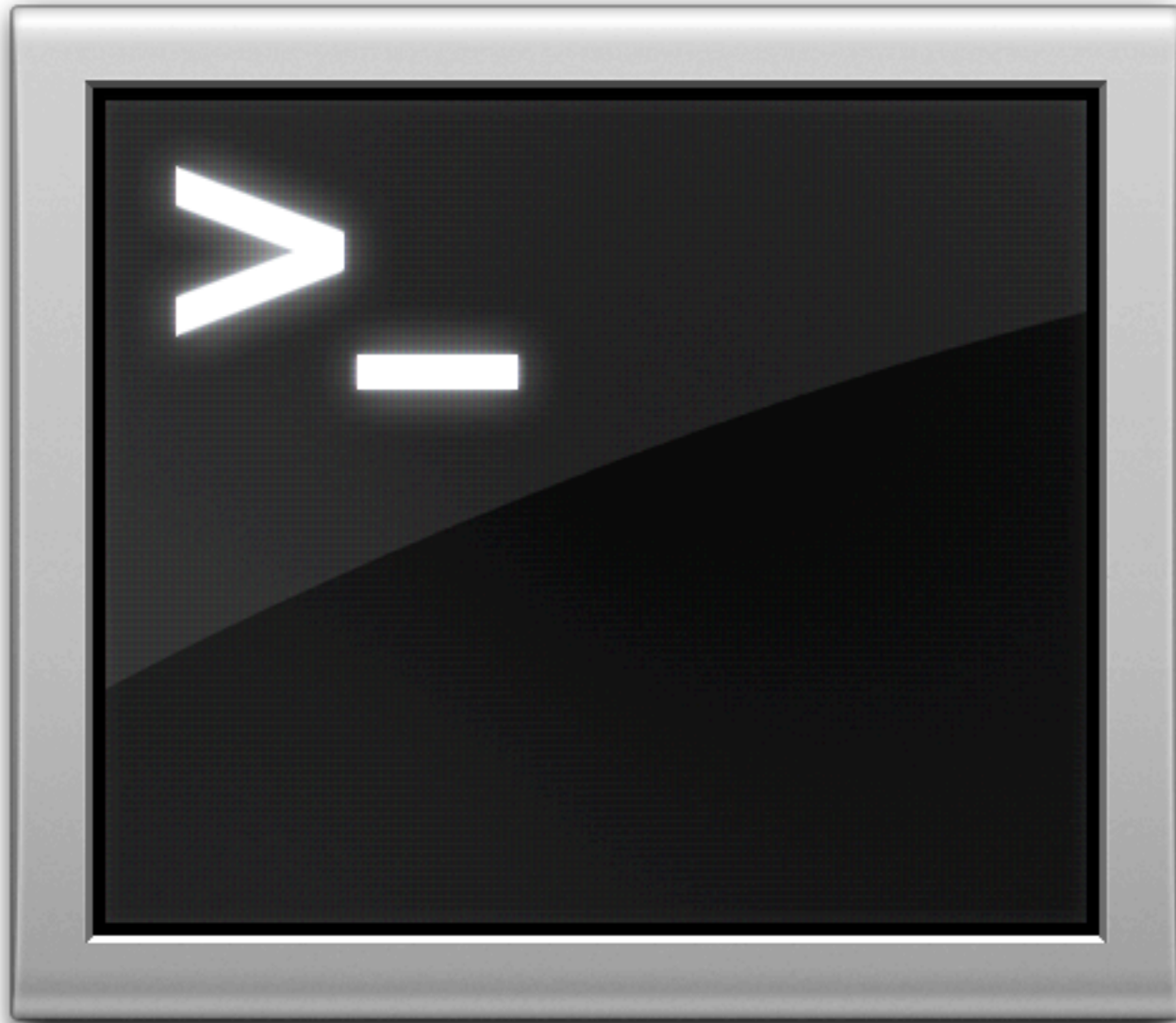
fdsetup remove -uuid

sudo fdsetup remove -uuid uuid_here

A terminal window with a title bar that reads "rtrouton — bash — 89x5". The window contains two lines of text: "troutont-vm1:~ rtrouton\$ sudo fdsetup remove -uuid C8F2BB40-3949-4A51-B283-B37DE478D660" and "troutont-vm1:~ rtrouton\$". A cursor is visible at the end of the second line.

```
troutont-vm1:~ rtrouton$ sudo fdsetup remove -uuid C8F2BB40-3949-4A51-B283-B37DE478D660
troutont-vm1:~ rtrouton$
```

fdsetup sync



› Compares directory service account information with Mac's list of FileVault 2 enabled accounts

- Removes users that have been removed from the directory service.
- Does not add directory service accounts to list of FileVault 2 enabled accounts.

New in 10.8.2: fdsetup authrestart



fdsetup = FileVault 2 multi-tool



Additional information



Additional information



Apple Technical White Paper

Best Practices for Deploying FileVault 2

Deploying OS X Full Disk Encryption Technology

August 2012 – OS X 10.7.4

Links

- Apple Best Practices for Deploying FileVault 2 - <http://training.apple.com/osx>
- Using fdesetup with Mountain Lion's FileVault 2 - <http://derflounder.wordpress.com/2012/07/25/using-fdesetup-with-mountain-lions-filevault-2/>
- Embedding certificate data into a fdesetup plist file - <http://derflounder.wordpress.com/2012/08/22/embedding-certificate-data-into-a-fdesetup-plist-file/>
- Encrypting Volumes in OS X Mountain Lion - <http://krypted.com/mac-os-x/encrypting-os-x-mountain-lion/>

Downloads

**PDF available from the
following link:**

<http://tinyurl.com/mt2012fv2PDF>

**Keynote slides available
from the following link:**

<http://tinyurl.com/mt2012fv2keynote>

**Thank you
for attending!**

**Enjoy the rest of the
conference**

@rtrouton

FOLLOW ME ON **twitter**