



SAMPLE PAGES

Mac in the Enterprise IT Configuration Guide

For Your Mac Evaluation and
Deployment

(Version 5.0)



SAMPLE PAGES

Table of Contents

Introduction	1
1 Imaging	2
1.1 Imaging Mac Computers	2
1.2 Creating Packages.....	3
1.2.1 Creating Packages with PackageMaker	4
1.2.1.1 Creating a Snapshot Package with PackageMaker.....	10
1.2.2 Creating Packages Using Third-Party Utilities.....	16
1.3 Creating Images with System Image Utility	17
1.3.1 NetInstall from Installer.....	18
1.3.2 NetRestore from Installer	21
1.3.3 Using NetRestore from a Prepared Volume.....	24
1.3.4 Creating NetRestore NetBoot Sets	27
1.3.5 Automations with System Image Utility	30
1.3.5.1 Creating an External OS X Recovery Volume	38
1.3.5.2 Adding Updates	39
1.3.5.3 Adding Post-Install Scripts.....	40
1.3.5.4 Adding Additional Software	41
1.3.5.5 Adding Configuration Profiles.....	42
1.3.5.6 Advanced System Image Utility Preferences	43
1.4 Creating an Image with a Configured Mac.....	44
1.4.1 Preparing a System for Imaging.....	45
1.4.1.1 Removing Unneeded LKDC Information	46
1.4.1.2 Removing .DS_Store Files	48
1.4.1.3 Removing Other System Files	49
1.4.2 Customizing the Default User Template.....	50
1.4.3 Self-Removing Scripts	51
1.5 Creating Images with Disk Utility	53
1.5.1 Creating a Disk Image from the Command Line.....	57
2 Deployment	58
2.1 Local Deployment	58
2.1.1 Creating a Bootable Disk or Volume Using NetInstall	59
2.1.2 Deploying Images with Disk Utility	61
2.2 NetInstall Image Creation	62
2.2.1 Configuring a NetInstall Server.....	65
2.2.2 Booting to a NetInstall Image	72
2.2.3 Unicast Apple Software Restore.....	74
2.2.4 Multicast Apple Software Restore	75
2.2.5 Third-Party Deployment Solutions.....	77
2.2.6 Setting Clients to NetBoot Using the bless Command	78
2.2.7 Using NetBoot DHCP Helpers	79
2.2.8 bootpd Relay	80
2.3 Minimal Touch Deployments.....	81

SAMPLE PAGES

3	Support and Maintenance	82
3.1	Asset Tags	82
3.2	Apple Remote Desktop	83
3.2.1	Apple Remote Desktop and Computer Lists	84
3.2.2	Deploying Applications	88
3.2.3	Inventory Tools	92
3.2.4	Apple Remote Desktop Task Server	94
3.3	Software Update Policy	96
3.4	OS X Server Software Update Service	98
3.4.1	Configuring Software Update Server Clients	101
3.4.2	Cascading Software Update Services	103
3.5	Third-Party Software Update Services	105
3.6	Client Management Suites	106
4	Directory Services	107
4.1	Local Directory Services	108
4.1.1	Creating Local Administrative Accounts	110
4.1.1.1	Creating Local Administrative Accounts Using System Preferences	111
4.1.1.2	Creating a Local Administrative Account Using the Command Line	114
4.1.1.3	Hiding a Local Account	116
4.1.1.4	Changing the Local Administrative Account	117
4.1.2	Nesting Network Administrators in a Local Administrative Group	118
4.1.3	Creating a Local Administrative Account with a Package or Script	120
4.2	Open Directory	121
4.2.1	Setting Up an Open Directory Master	122
4.2.2	Preparing to Bind to Open Directory	128
4.2.2.1	Binding to Open Directory Using the Users & Groups Pane in System Preferences	130
4.2.2.2	Custom Binding Operations	134
4.2.3	Binding to Open Directory Using the Command Line	143
4.2.4	Binding to Open Directory Using a Post-Installation Script	145
4.2.5	Using Server to Create New Users and Groups	146
4.2.6	Setting Up an Open Directory Replica	152
4.3	Active Directory	155
4.3.1	Binding to Active Directory	156
4.3.1.1	Binding to Active Directory Using Directory Utility	157
4.3.1.2	Testing and Verifying Active Directory Binding Information	162
4.3.1.3	Binding to Active Directory from the Command Line	167
4.3.1.4	Binding to Active Directory Using a Script	170
4.3.1.5	Binding to an Active Directory Using a Post-Install Script	171
4.3.1.6	Active Directory Plugin Troubleshooting Commands	172
4.3.2	Mapping the UID and GID with Directory Utility	176
4.3.2.1	Mapping UID, User GID, and Group GID Using dsconfigad	181
4.3.3	Setting a User Home Directory	182
4.3.4	Namespace Support	187
4.3.5	Active Directory Packet Encryption Options	188
4.3.6	SSL Binding Instructions	190
4.3.7	Managing Certificates from the Command Line	192
4.3.8	Active Directory Computer Password Changes	193
4.4	Third-Party Active Directory Plugins	194

SAMPLE PAGES

4.5	LDAP	195
4.5.1	Binding to LDAP	196
4.5.1.1	Simple Binding	197
4.5.1.2	Trusted Bind.....	201
4.5.2	Mapping LDAP Attributes	205
4.6	NIS	213
4.7	Kerberos.....	217
4.8	Distributed File Sharing (DFS).....	218
4.8.1	Connecting to DFS Shares	219
4.8.2	Viewing DFS Shares with smbutil.....	220
4.8.3	Third-Party DFS Solutions.....	222
5	Policy Management	223
5.1	Setting up a Profile Manager Server	223
5.1.1	Configuring Network Settings.....	224
5.1.2	Configuring Users	228
5.1.3	Adding Groups.....	230
5.1.4	Reviewing Certificates	233
5.1.5	Acquiring Apple Push Notification Certificates	237
5.1.6	Enabling Profile Manager	241
5.1.7	Automatic Push Versus Manual Download Profiles.....	247
5.1.8	Editing Management Profiles.....	248
5.1.9	Creating Device Groups	252
5.1.10	Using Device Placeholders.....	255
5.1.11	Enrolling OS X Devices	258
5.1.12	Locking a Device via the User Portal	263
5.1.13	Wiping a Device via the User Portal.....	265
5.1.14	Locking a Device Using Profile Manager	267
5.1.15	Wiping a Device Using Profile Manager	270
5.1.16	Removing a Mac from Management via the User Portal	273
5.1.17	Removing Management via Profile Manager.....	275
5.1.18	Profile System Preferences	277
5.1.19	Forcing Management Profiles.....	279
5.1.20	profiles Command.....	282
5.2	Managing Profiles	283
5.2.1	Viewing the Contents of Profiles	284
5.2.2	Configuring the Location of the Dock	285
5.2.3	Managing Third-Party Application Preferences.....	289
5.2.4	Managing Printers.....	294
5.2.5	Using Profile Manager to Whitelist Applications	298
6	Security	303
6.1	Security Resources.....	303
6.2	Application Restrictions	303
6.2.1	Application Launch Security	304
6.3	Password Policies	307
6.3.1	Auditing Local Password Policies	310
6.3.2	Setting Local Password Policies	313
6.4	Setting an Open Firmware Password	314
6.5	Remote Login.....	315
6.5.1	Key-Based SSH Access	317

SAMPLE PAGES

- 6.6 FileVault.....319
 - 6.6.1 Enabling FileVault from the Command Line328
 - 6.6.2 Master Passwords.....329
- 6.7 Third-Party Full Disk Encryption.....331
- 6.8 Network Firewall.....332
 - 6.8.1 Application Layer Firewall333
 - 6.8.1.1 Configuring the Application Layer Firewall.....334
 - 6.8.1.2 Managing the Application Layer Firewall from Terminal338
 - 6.8.2 pf.....340
 - 6.8.3 ipfw (deprecated).....342
- 6.9 Keychain Usage and Management.....344
 - 6.9.1 Accessing and Viewing Keychain Contents345
 - 6.9.2 Selecting Specific Categories of Keychain Items347
 - 6.9.3 Enabling Directory Services Searching for Certificates348
 - 6.9.4 Enabling Certificate Revocation Checking349
 - 6.9.5 Importing Items into a Keychain via the GUI.....351
 - 6.9.6 Importing Items into a Keychain from within Keychain Access.....353
 - 6.9.7 Exporting Items from a Keychain356
 - 6.9.8 Exporting Items from a Keychain via the GUI.....358
- 6.10 Encrypted Time Machine Backups.....359
- 6.11 Third-Party Smart Card Service Options.....364
- 7 Networking/Wireless365**
 - 7.1 IPv4 Networking.....366
 - 7.2 IPv6 Networking.....376
 - 7.3 Network Setup Assistant for Wired and Wireless.....380
 - 7.4 Network Diagnostics for Wired and Wireless385
 - 7.5 VLAN Wired Network Deployment389
 - 7.6 Networking Command Line Interface (CLI)394
 - 7.7 VPN.....402
 - 7.8 Network Security Overview417
 - 7.8.1 WPA / TKIP — PSK.....418
 - 7.8.2 WPA2 / AES — PSK.....420
 - 7.8.3 WPA2 / AES 802.1x — PEAP / MSCHAPv2422
 - 7.8.4 WPA2 / EAS 802.1x — EAP-TLS429
 - 7.8.5 WPA2 / AES 802.1x — TTLS438
 - 7.8.6 WPA2 / AES 802.1x — EAP-FAST447
 - 7.9 Importing and Exporting 802.1x Profiles456
 - 7.10 802.1x Operation for Networking.....459
 - 7.11 Obtaining a Certificate from a Windows CA.....461
 - 7.12 Trusting Certificates from the Command Line.....464
- 8 Collaboration465**
 - 8.1 Microsoft Exchange Integration.....465
 - 8.1.1 Using Mail, Calendar, and Contacts with Exchange.....466
 - 8.1.2 Enabling S/MIME in Mail.....469
 - 8.1.3 Enabling Out of Office in Mail.....470
 - 8.2 Connecting to and Troubleshooting Mail, Calendar, and Contacts with Microsoft Exchange472
 - 8.2.1 DNS473
 - 8.2.2 Improper Redirects / Certificate Errors474

SAMPLE PAGES

8.2.3	Limiting Message Size	475
8.2.4	Additional Troubleshooting Resources	477
8.3	Troubleshooting Outlook 2011	478
8.3.1	Additional Outlook 2011 Information	480
8.4	Connecting to SharePoint	481
8.4.1	Additional SharePoint Information	484
8.5	Instant Messaging.....	485
8.5.1	Messages and FaceTime.....	486
8.5.2	Lync Server 2010	490
8.6	AirDrop	494
8.6.1	Deactivating AirDrop	496
8.6.2	Debugging AirDrop	500
8.6.3	Additional AirDrop Information	501
8.7	iCloud.....	502

© 2012 Apple Inc. All rights reserved.

Apple, the Apple logo, AirPort, Bonjour, Boot Camp, FaceTime, FileVault, Finder, FireWire, iPad, iPhone, iPod touch, iTunes, Keychain, Mac, the Mac logo, Mac Pro, MacBook, MacBook Air, Mountain Lion, OS X, Safari, Spotlight, Time Machine, and Xcode are registered trademarks of Apple Inc., registered in the U.S. and other countries. Apple Remote Desktop, Launchpad, and iMessage are trademarks of Apple Inc. App Store is a service mark of Apple Inc., registered in the U.S. and other countries. iCloud is a registered service mark of Apple Inc., registered in the U.S. and other countries. Intel and Thunderbolt are trademarks of Intel Corp. in the U.S. and other countries. FileMaker is a registered trademark of FileMaker Inc. in the U.S. and other countries. UNIX is a registered trademark of The Open Group. The Bluetooth® word mark is a registered trademark owned by Bluetooth SIG, Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use.

SAMPLE PAGES

Introduction

This configuration guide is designed to help IT professionals evaluate and deploy OS X on Mac computers in medium to large organizations. Each section contains modules that cover different topics with step-by-step instructions. Using this guide, organizations can accelerate testing and planning to begin a proof of concept, or a broader end-user deployment, of Mac computers.

This guide was developed as a reference document. Not all modules are required reading for every Mac deployment plan. It covers a wide range of topics critical to successfully deploying Mac systems including:

- Imaging
- Deployment
- Support and Maintenance
- Directory Services
- Policy Management
- Security
- Networking/Wireless
- Collaboration

Before using this guide, consult with your Apple sales representative or Apple Authorized Reseller for assistance determining the right modules for your environment.

SAMPLE PAGES

1 Imaging

1.1 Imaging Mac Computers

The first step in deploying most systems, including those running OS X, is to create disk images for deployment. Apple includes robust imaging tools that can be used on their own or in conjunction with third-party tools to create images. More important than the tools themselves, however, is how they're used.

A wide range of imaging strategies are available, and administrators can choose between various methodologies for creating deployment images. A traditional monolithic-system imaging approach works well for small proof of concept deployments, allowing for rapid deployment and user testing. However, to properly scale, production deployments should leverage the power of programmatic, or modular, image creation workflows. In these situations, deployment images are required to rapidly deploy systems en masse.

This section includes modules about the tools and techniques for creating OS X deployment images.

SAMPLE PAGES

1.2 Creating Packages

Imaging often includes packaging software for distribution. OS X offers a number of tools for creating installation packages and package distribution.

Most application installers place files on a file system, files that interact with the operating system in some way. A package is a file, or bundle of files, with a “.pkg” extension. The package bundle contains an archive of files to install, scripts that perform specified actions (which can run before or after file archives are placed into the destination they’re bound for), and information about how the operating system should interpret the installer (such as the order in which these operations occur). A package can also include licensing documents and other information.

Packages have a number of uses related to installing and managing software. For example, application developers often use packages to build installers for their software. Apple uses packages to provide system or application upgrades using Software Update. Administrators often use packages to deploy scripted changes to client systems, such as binding to a directory service.

A meta package, which has a “.mpkg” file extension, is a set of packages that are distributed in one structure. The meta package typically provides a list of checkboxes that can be used to choose which packages or components of a larger installation framework are installed.

To install a package, double-click its icon in the Finder. The Installer application opens and guides you through the necessary steps of the installation, defined at the time the package was created. Packages can also run silently through the command line, with Apple Remote Desktop, or using third-party patch management software solutions.

Many applications come bundled as standard Apple Installer packages. In situations where an application installer is already a package, custom packages may not be required. Vendors that distribute packages often have a process for preparing a package for mass deployment (such as instructions on embedding license keys). Contacting the vendor can save valuable time, minimize the amount of user interaction required to install a package, and help prevent unintended consequences.

Packages can be created using a number of tools. The most notable tool is PackageMaker, which is available from the Apple website (www.apple.com). Packages can be built manually or using a snapshot of the operating system. Snapshot-based packages are great for those new to building packages. However, when using a snapshot-based package creation tool, keep in mind that extraneous data may be unintentionally captured if changes unrelated to installation take place between snapshots. To avoid this, always review the files and folders to be installed when making a snapshot and remove those not required.

The process is similar to creating installers for other operating systems. Therefore, if a team member is already trained in creating installers for Microsoft Windows (that is, “.msi” or “.mst” installers) or Linux, it should be easy for them to quickly grasp the concepts needed to build packages in OS X.

SAMPLE PAGES

4.3 Active Directory

Active Directory is Microsoft's directory services solution. Active Directory provides information on users, groups, and computers (information stored in LDAP), password management and encryption (using Kerberos), and the ability to find objects on a network. Information in Active Directory is used to manage users, computers, groups, printers, and other resources. Administrators can also assign policies to Windows computers using Group Policy Objects.

Active Directory deployments vary from smaller environments with a few hundred objects to larger environments with thousands (or millions) of users and systems distributed across a number of sites.

Mac computers can be manually bound to Active Directory through the Active Directory module in Directory Utility. From the command line, use `dsconfigad` to bind and specify Active Directory-specific options.

This section contains modules that explore the administrative tasks surrounding the management of OS X using Active Directory.

SAMPLE PAGES

4.3.1 Binding to Active Directory

OS X is bound to Active Directory from the Users & Groups pane in System Preferences; through Directory Utility (located in /System/Library/CoreServices/Directory Utility); or using the command-line utility `dsconfigad`. While `dsconfigad` does contain some additional options, the majority of functionality is available through Directory Utility, so no command-line options are required for everyday use.

To perform Active Directory validation:

Prior to binding, it's important to verify some connectivity with Active Directory. Because Active Directory clients use DNS service records to locate Active Directory service, it's important to verify that DNS is working properly.

1. Open Terminal from /Applications/Utilities. Enter the following command to do a lookup on the service record to locate the global catalog:

```
dig -t SRV _gc._tcp.pretendco.com
; <<>> DiG 9.4.1-P1 <<>> -t SRV _gc._tcp.pretendco.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34512
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; QUESTION SECTION:
_gc._tcp.pretendco.com.          IN      SRV

;; ANSWER SECTION:
_gc._tcp.pretendco.com.        600     IN      SRV      0 100 3268
dc.pretendco.com.

;; ADDITIONAL SECTION:
dc.pretendco.com. 3600     IN      A        192.168.55.47

;; Query time: 83 msec
;; SERVER: 192.168.1.6#53(192.168.55.47)
;; WHEN: Thu Jul 31 14:09:32 2008
;; MSG SIZE rcvd: 92
```

2. If the response doesn't include an answer section with the name of a domain controller, check to make sure the OS X network settings are correct and that the DNS specified is one that will return service record information for your Active Directory forest.
3. To bind OS X to Active Directory, you need credentials as a local administrator on the Mac as well as an Active Directory user who has the authority to join computers to the Organizational Unit (OU) that you'll be leveraging in Active Directory.

Once bound to Active Directory, set up the client to allow Active Directory administrators (or any Active Directory user you choose) to be local administrators on the local Mac client. This isn't done automatically.

During initial setup, you'll need the local administrative user name and password for the Mac. This user is the first user set up during Setup Assistant after installation or a local administrative account created on the system during imaging.

SAMPLE PAGES

4.3.1.1 Binding to Active Directory Using Directory Utility

To bind to Active Directory using Directory Utility:

1. Choose System Preferences from the Apple menu.
2. Open the Users & Groups pane.



Figure 4.3.1.1_1

3. Click Login Options.

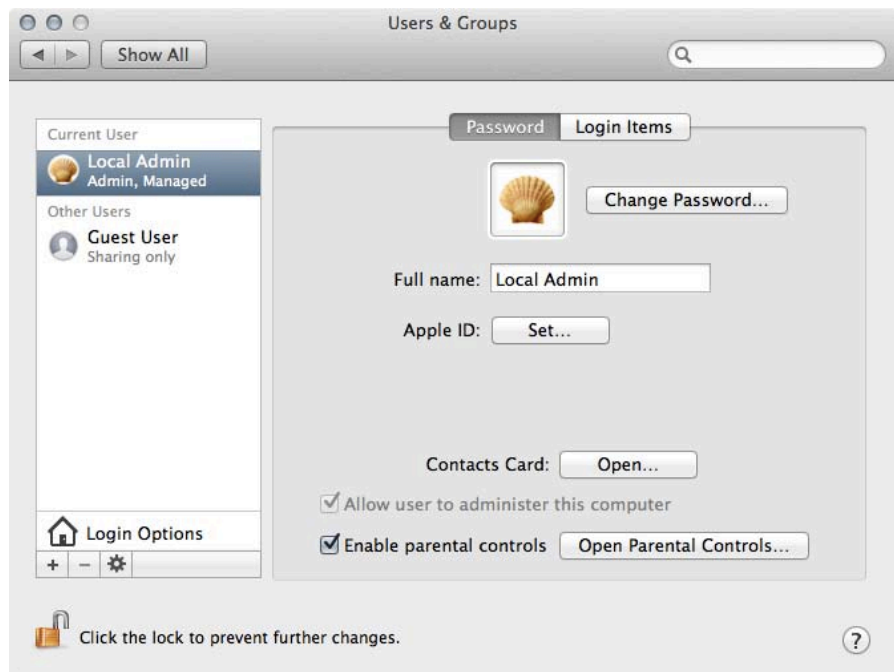


Figure 4.3.1.1_2

SAMPLE PAGES

4. Click Join to the right of Network Account Server.

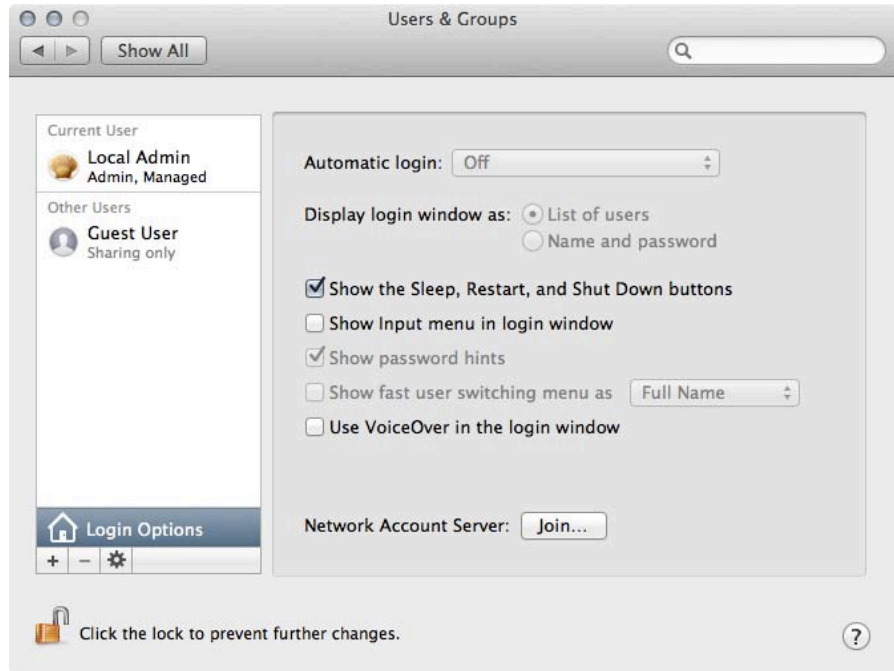


Figure 4.3.1.1_3

5. Enter the name of the domain in the Server field. The dialog expands for credentials and Computer ID, which is already entered.

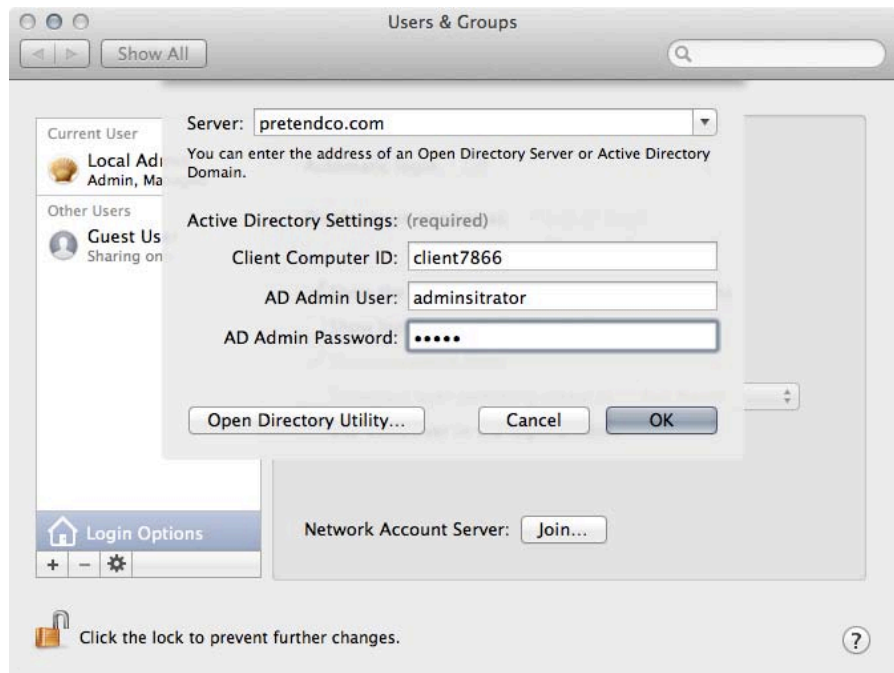


Figure 4.3.1.1_4

SAMPLE PAGES

6. Once joined, review the binding information and provide more details, if needed. You can also access the Active Directory options in Directory Utility to bind, if more information is required at the bind screen. To open Directory Utility, click the Edit button in the Users & Groups pane in System Preferences (or if the initial attempt at binding failed, click Join).
7. Click the Open Directory Utility button.

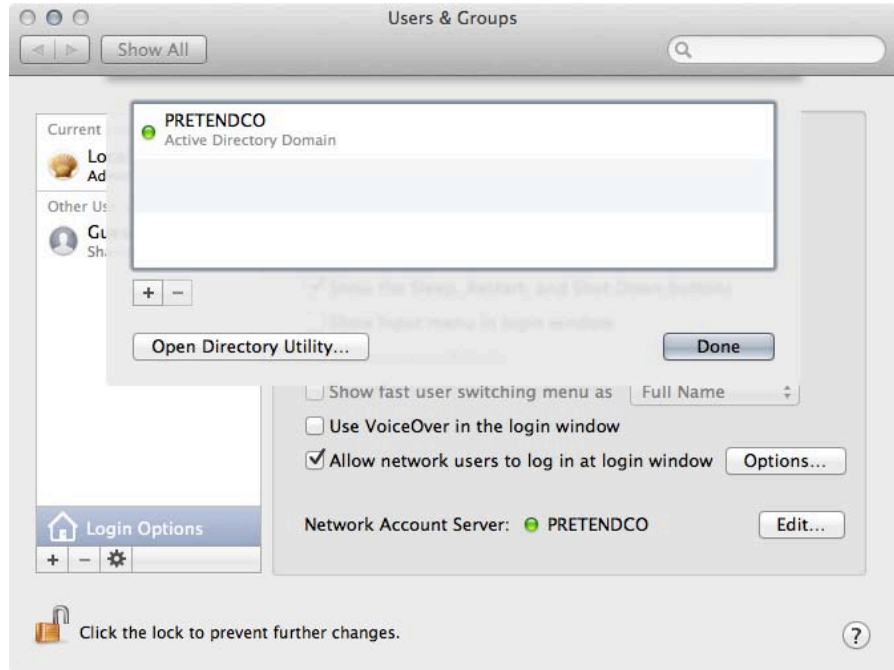


Figure 4.3.1.1_5

SAMPLE PAGES

8. Double-click Active Directory (or click Active Directory, then the pencil icon).

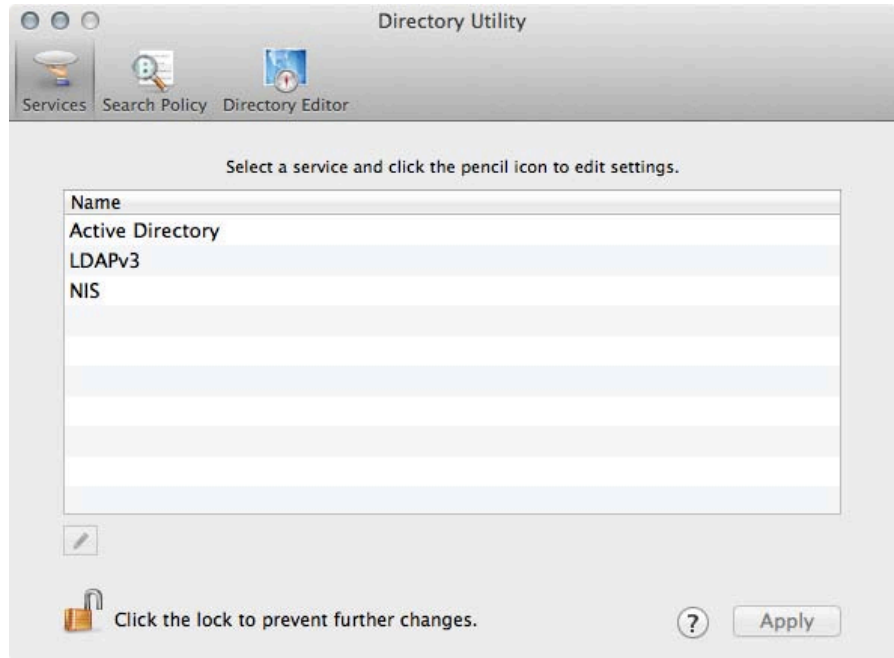


Figure 4.3.1.1_6

9. Enter the Active Directory domain name to join (if you've not yet bound).
10. Change the computer ID if necessary, and click OK.

Note: When the system is bound, you'll see an Unbind button.

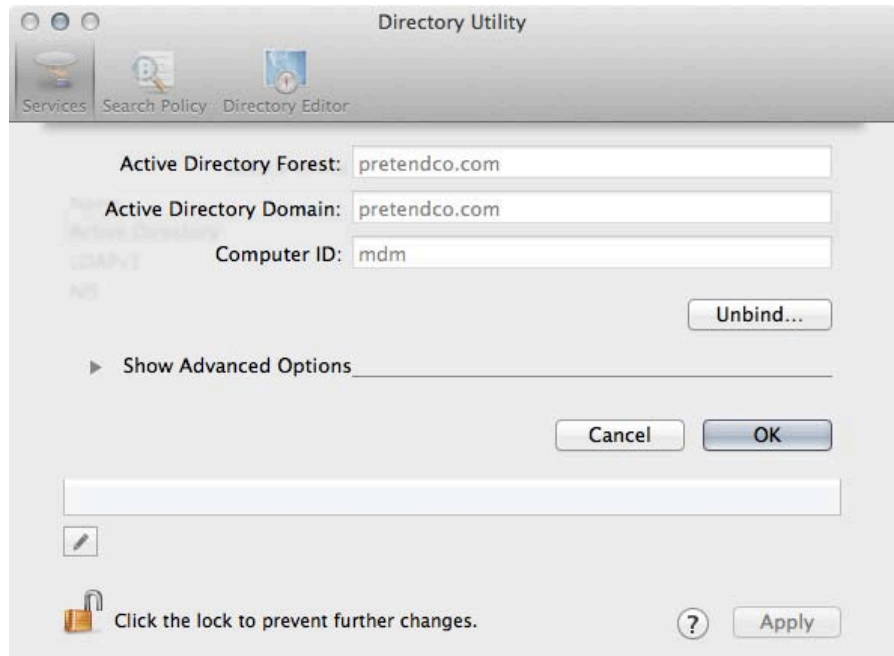


Figure 4.3.1.1_7

SAMPLE PAGES

11. If binding, enter the Active Directory user that has the delegated authority to bind a machine to the OU you specify for Computer OU.
12. Enter the Active Directory user's password, then click OK.
13. In the Users & Groups pane in System Preferences, a green light next to the domain indicates that network accounts are accessible.

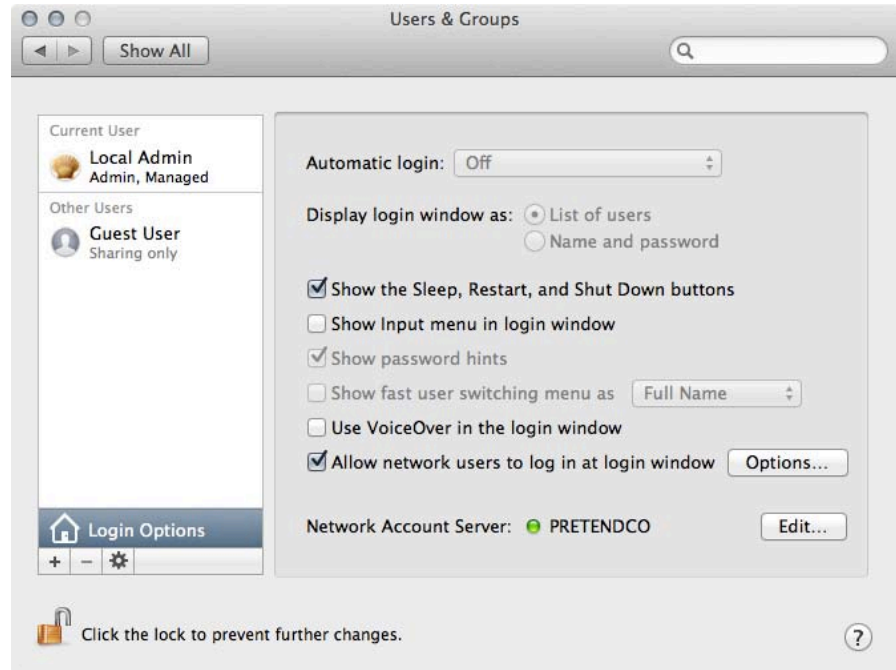


Figure 4.3.1.1_8

SAMPLE PAGES

4.3.1.2 Testing and Verifying Active Directory Binding Information

Prior to logging out and attempting to log in with an Active Directory user, verify that OS X is getting the requisite information from Active Directory.

This section shows how to verify that OS X is able to get information about an Active Directory user, browse information within Active Directory, and authenticate users.

To verify that the Mac can get information about an Active Directory user:

For OS X to work correctly, it needs to be able to look up information such as the user's numerical ID (UID), primary group ID (GID), and group membership.

1. To test this lookup capability, open Terminal from /Applications/Utilities, and enter the following:

```
id <Active Directory Username>
```

Sample:

```
Client-1:~ admin$ id jfoster
```

```
uid=818406992(jfoster) gid=1450179434(PRETENDCO\domain users) groups=1450179434(PRETENDCO\domain users)
```

2. If the `id` command does not return information about an Active Directory user, open Directory Utility and verify that OS X is bound to Active Directory, and that Active Directory is listed under Search Path (the listing is created automatically when the client is bound). Also verify network connectivity between OS X and the domain controller, and check firewall settings on the network.

To browse the Active Directory network node:

1. Open Terminal from /Applications/Utilities, and enter the following:

```
Client-1:~ admin$ dscl localhost
```

```
>
```

2. You're now in interactive mode and can browse network nodes, which are logical representations of disparate directory services. Type `ls` to see a list of types:

```
> ls
```

One of the listed nodes is Active Directory (if not, Active Directory isn't enabled in Directory Utility).

```
Active Directory
```

```
BSD
```

```
Local
```

```
Search
```

```
Contact
```

SAMPLE PAGES

3. Navigate into the Active Directory node using `cd` and perform another `ls` to show the contents of the node.

```
> cd 'Active Directory'
/Active Directory > ls
All Domains
```

4. Navigate into the All Domains node by using `cd`, and perform another `ls` to show the contents of the node. The node should contain the Users node.

```
/Active Directory > cd 'All Domains'
/Active Directory/All Domains > ls
CertificateAuthorities
Computers
FileMakerServers
Groups
Mounts
People
Printers
Users
```

5. Navigate into the Users node by using `cd`, and perform another `ls` to show the contents of the node. The node should contain all users in the forest. If you have a large number of users, don't enter `ls` to list the contents of this node. Instead, use `read` to read the attributes of that user:

```
/Active Directory/All Domains > cd Users
/Active Directory/All Domains/Users > read jfoster

dsAttrTypeNative:accountExpires: 9223372036854775807
dsAttrTypeNative:ADDomain: pretendco.com
dsAttrTypeNative:badPasswordTime: 0
dsAttrTypeNative:badPwdCount: 0
dsAttrTypeNative:cn:
  Tim Lee
dsAttrTypeNative:codePage: 0
dsAttrTypeNative:countryCode: 0
dsAttrTypeNative:displayName:
  Tim Lee
dsAttrTypeNative:distinguishedName:
  CN=Jimmy Foster,CN=Users,DC=pretendco,DC=com
more...
```

6. If the attributes of a user aren't listed, check access controls in Active Directory and verify that you've bound to the correct OU.
7. You can now exit out of `dscl`.

```
/Active Directory/All Domains/Users > exit

Goodbye
```

SAMPLE PAGES

5.1.19 Forcing Management Profiles

Management profiles are a policy enforcement system. When creating profiles in Profile Manager, administrators have options for controlling how those profiles can be removed.

The default removal setting is to always allow removal of a profile, which means a user profile can be removed by the user to which it applies. Device profiles can then be removed by any administrative user on a Mac. However, some policies should be enforced whether the user wishes to have them or not.

The Authorization feature secures profile removal, forcing a specific password to be used to edit a profile. Only users with the profile password may remove it.

The Never removal setting indicates that a profile may not be removed. The device must be wiped in order to remove the profile.

To change profile removal rules:

1. Open the Server application from /Applications.
2. Choose Profile Manager from the Services list in the sidebar.
3. Click Open Profile Manager in the Profile Manager pane.
4. Authenticate with the credentials for an administrative account.
5. Choose the User, Group, Device, or Device Group to edit.

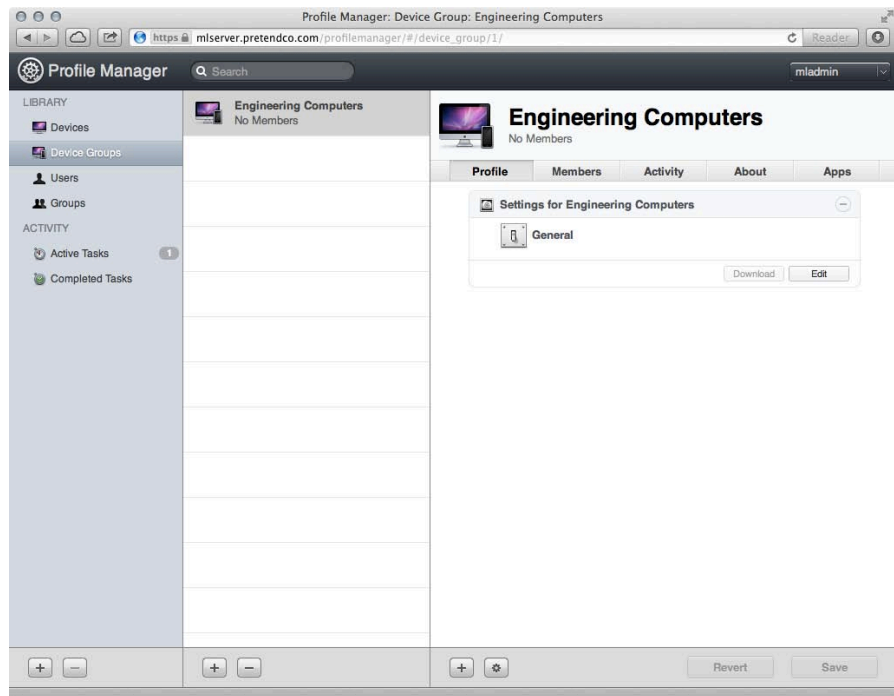


Figure 5.1.19_1

SAMPLE PAGES

6. Click the Edit button for the profile.

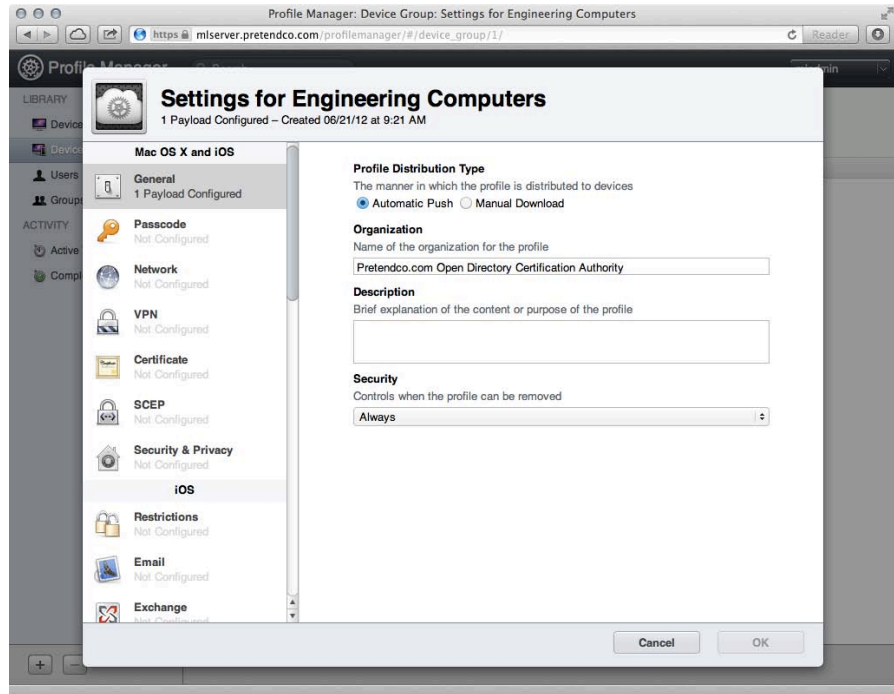


Figure 5.1.19_2

7. Change the Security settings for the profile as needed.

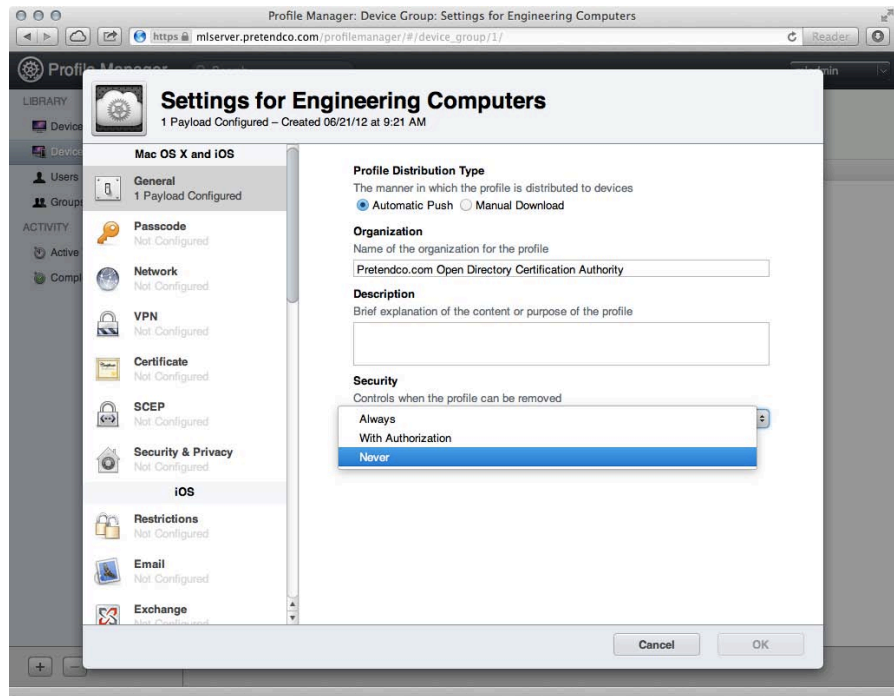


Figure 5.1.19_3

SAMPLE PAGES

8. Set any other settings that should be deployed with the profile.
9. Click OK to close the Settings pane.
10. Click Save to update the profile settings.

SAMPLE PAGES

5.1.20 profiles Command

The `profiles` command allows programmatic control of configuration profiles, so, administrators can script or remotely run configuration profile installation, removal, and auditing. To list the configuration profiles installed for a given user, run the `profiles` command with the `-L` option, as follows:

```
profiles -L
```

To see all configuration profiles installed on the system, run the `profiles` command with the `-P` option, as follows:

```
profiles -P
```

To install a configuration profile for a user, run the `profiles` command with the `-I` option (for *Install*), followed by the `-F` option (for *file*), and ending with the path to the profile file. For example, the following command installs a configuration profile called `8021xSetup.mobileconfig` previously copied to `/tmp`.

```
profiles -I -F /tmp/8021xSetup.mobileconfig
```

To remove that profile, use the following command:

```
profiles -R -F /tmp/8021xSetup.mobileconfig
```

An effective way to troubleshoot profile problems is to remove all configuration profiles using the `-D` option, as follows:

```
profiles -D
```

Profiles installed from a Profile Manager instance are tracked using unique identifiers similar to a default domain. For example, if an organization is called `pretendco` and the profile to install is for 802.1x configuration, that profile might be called `com.pretendco.8021xSetup`. To remove this profile, use the `-R` option followed by `-p` to denote a profile, as follows:

```
profiles -R -p com.pretendco.8021xSetup
```

To see the version number of the `profiles` command, use the `-x` option:

```
profiles -x
```

See the `man` page for `profiles` for more information, using the following command:

```
man profiles
```

SAMPLE PAGES

6.6 FileVault

FileVault 2 offers full disk encryption for data-at-rest (DAR) protection and is built into OS X. FileVault 2 keeps all files on a Mac secure, even if the computer is lost or stolen, using XTS-AES-128 (256-bit keys) data encryption at the disk level.

FileVault 2 protects sensitive information on a Mac and is particularly well suited for notebooks that could be lost or stolen. With FileVault 2 turned on, all information on the computer is kept safe from unauthorized access.

In this module, enable FileVault 2 full disk encryption.

To enable FileVault:

1. Open System Preferences from the Apple menu.
2. Click Security & Privacy.

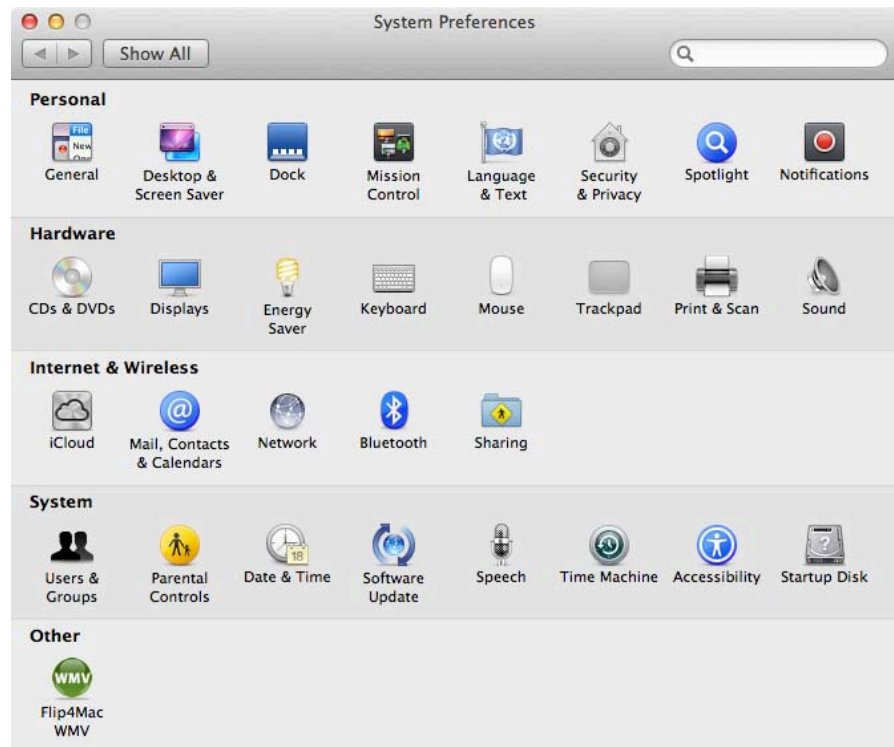


Figure 6.6_1

SAMPLE PAGES

3. Click FileVault. **Note:** If an older version of FileVault was enabled prior to upgrading to OS X Mountain Lion, a button will be presented to Turn Off Legacy FileVault, as described in section 6.6.1.



Figure 6.6_2

4. Click the Turn On FileVault button.

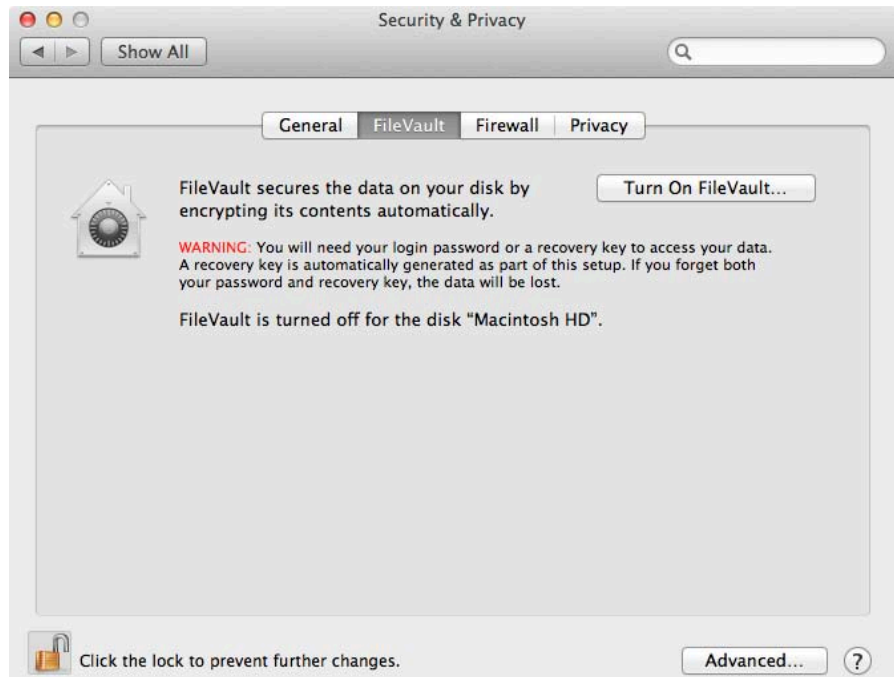


Figure 6.6_3

SAMPLE PAGES

5. If the system has multiple users, click Enable User for each authorized user. Then have the user enter his or her login password. Users who've provided passwords will be shown with a checkmark, while users who still require a password will be shown with an Enable User button. Users who don't have any password set will be shown with a Set Password button.

Note: Logging in after the system disk has been unlocked by another user is still possible, even if the user isn't enabled here.



Figure 6.6_4

SAMPLE PAGES

6. When prompted, provide the password.
7. Click Continue once all authorized users are enabled.

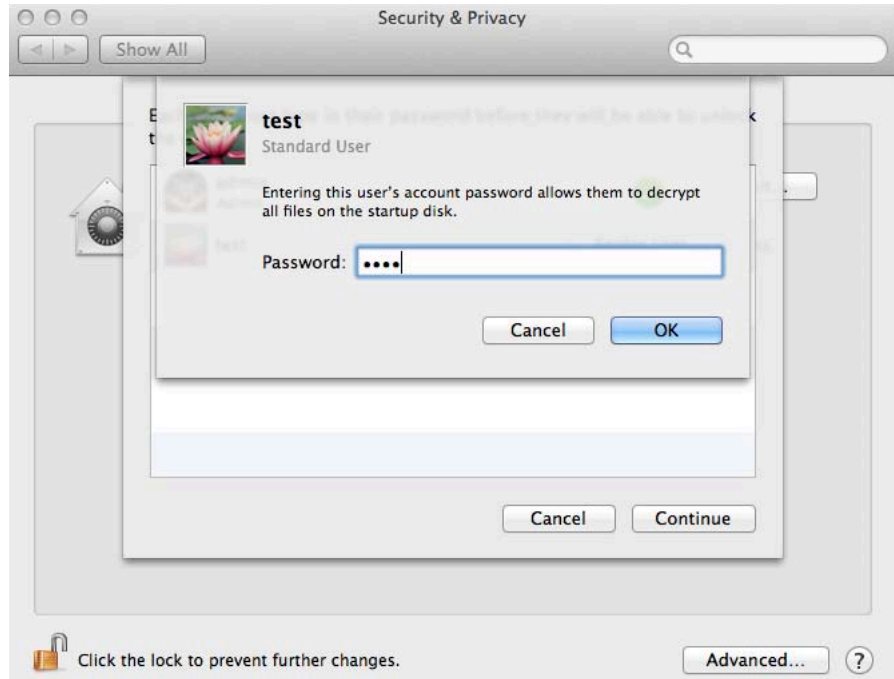


Figure 6.6_5

8. At the Recovery Key screen, document the displayed recovery key.
9. Click Continue.

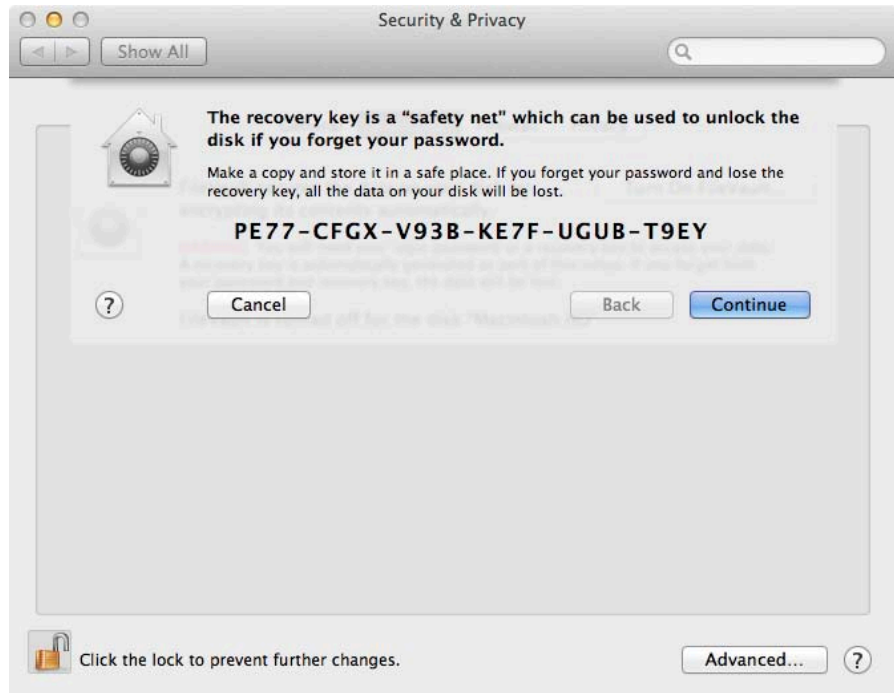


Figure 6.6_6

SAMPLE PAGES

10. (Optional) Choose to store the recovery key with Apple:
 - a. Click “Store the recovery key with Apple” to store the protected key on Apple servers.
 - b. Select three security questions to which you’ll always remember the responses.
 - c. Provide your responses below each question. These will need to be the same responses in the event recovery keys need to be retrieved.
 - d. The recovery key will be wrapped by a key generated from the selected questions and responses.
11. Click Continue.



Figure 6.6_7

SAMPLE PAGES

12. Click Restart to restart the Mac and begin the encryption process.



Figure 6.6_8

To verify FileVault 2 full disk encryption status:

1. Open System Preferences from the Apple menu.

SAMPLE PAGES

2. Click Security & Privacy.

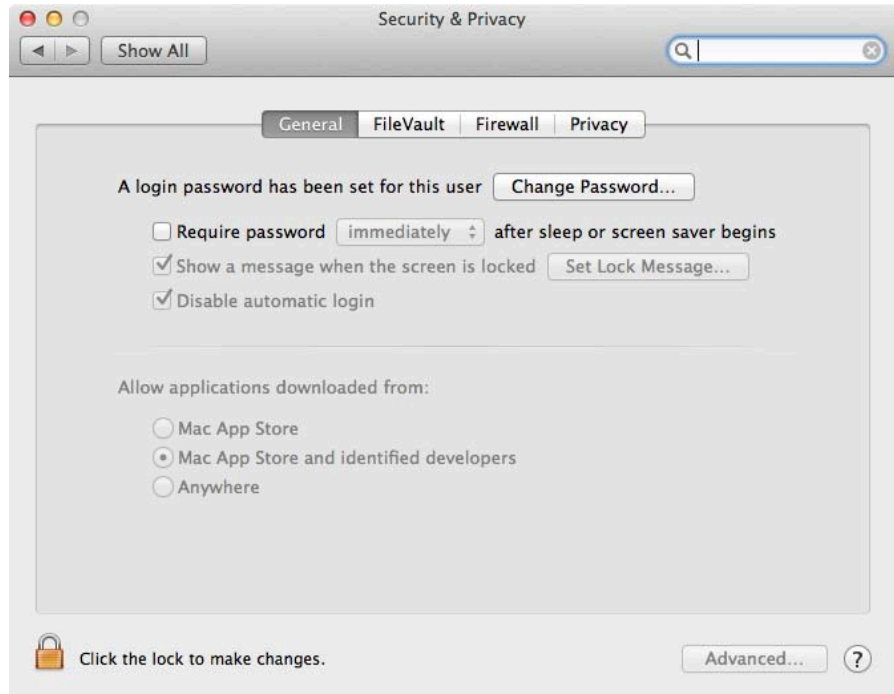


Figure 6.6_9

3. Click FileVault.



Figure 6.6_10

SAMPLE PAGES

4. Note FileVault status:
 - a. "FileVault is turned on for the disk <disk name>." indicates Full Disk Encryption (FDE) has been enabled for the disk.
 - b. "FileVault is turned off for the disk <disk name>." indicates FDE hasn't been enabled for the disk.
 - c. "A recovery key has been set." indicates the protected recovery key is stored on Apple servers.
 - d. Encryption Finished indicates the drive has completed the conversion process and is now fully encrypted.

To disable FileVault:

1. Open System Preferences from the Apple menu.
2. Click Security & Privacy.
3. Click FileVault.
4. Click the Turn Off FileVault button.

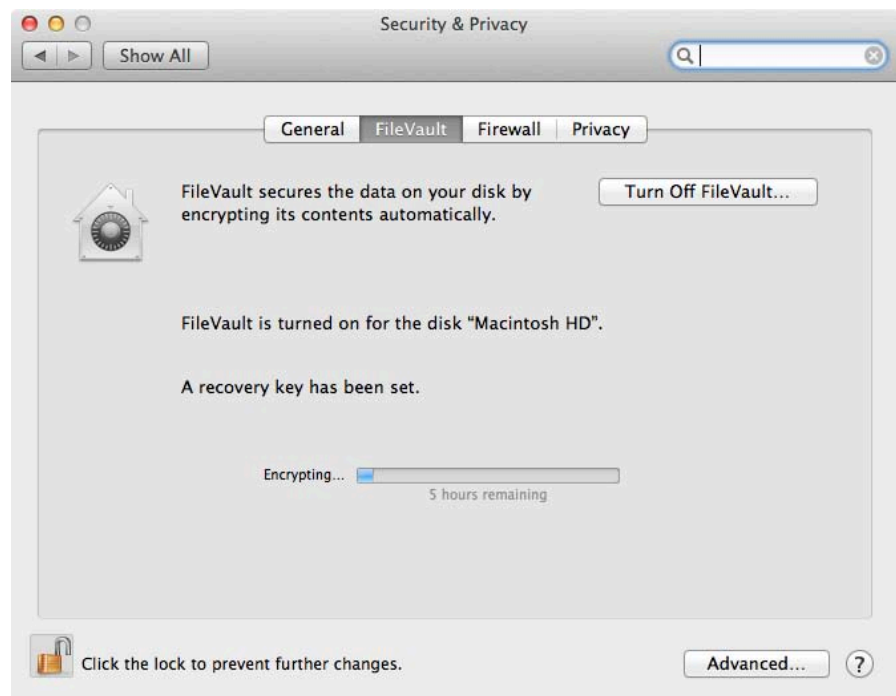


Figure 6.6_11

SAMPLE PAGES

5. Click Turn Off Encryption to confirm you wish to turn off FileVault.



Figure 6.6_12

SAMPLE PAGES

6.6.1 Enabling FileVault from the Command Line

OS X includes a command-line tool called `fdesetup` that allows system administrators to remotely manage FileVault. Use `fdesetup` to enable FileVault, disable FileVault, add and remove users that may unlock the volume, and determine whether FileVault is active on a particular Mac. In this module, use `fdesetup` to enable FileVault.

To enable FileVault from the command line:

1. Start a command-line session using Terminal or the Remote Login service.
2. Examine FileVault's current status by entering the command:

```
fdesetup status
```
3. After confirming FileVault is off, enable FileVault with the command:

```
fdesetup enable
```
4. Unless additional parameters are specified, an interactive session will prompt for the primary user's short name and password.
5. On enabling FileVault, a Recovery key is returned by the `fdesetup` command. It should be recorded or otherwise stored by IT.

SAMPLE PAGES

6.6.2 Master Passwords

Setting a Master Password to a value known by IT personnel is helpful in the event IT needs access to a FileVault encrypted Mac. It also helps with support when assistance is required and the Master Password is needed.

The FileVault Master Password is configured on a monolithic image for all clients concurrently. This keeps users from setting their own FileVault Master Password.

To set a FileVault Master Password in System Preferences:

1. Open System Preferences from the Apple menu.
2. Click Users & Groups.
3. Click the lock icon and authenticate to make changes.



Figure 6.6.2_1

4. Click the cog wheel icon and choose Set Master Password.

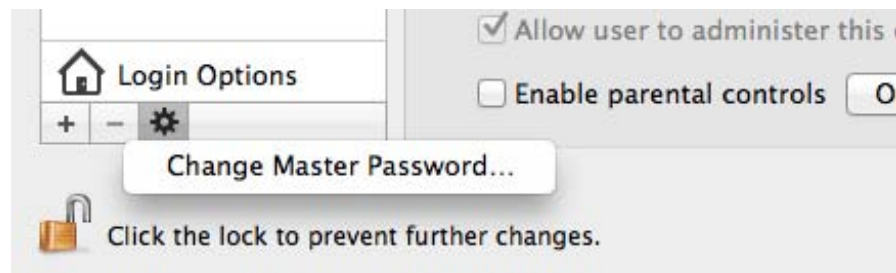


Figure 6.6.2_2

SAMPLE PAGES

5. Enter the desired Master Password.

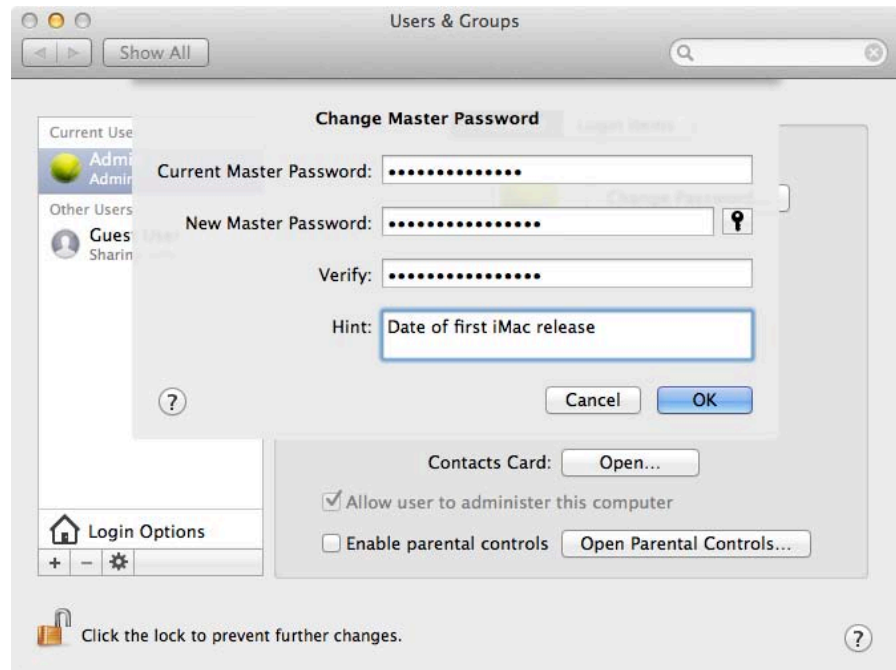


Figure 6.6.2_3

The Master Password is now set in a master image.