


Administering FileVault 2 on OS X Lion with the Casper Suite

Technical Paper
July 2012



 JAMF Software, LLC
© 2012 JAMF Software, LLC. All rights reserved.

JAMF Software has made all efforts to ensure that this guide is accurate.

JAMF Software
301 4th Ave S Suite 1075
Minneapolis, MN 55415-1039
(612) 605-6625

FileVault, the FileVault logo, Keychain Access, and Mac OS X are registered trademarks of Apple Inc., in the United States and other countries.

Casper Admin, the Casper Suite, Composer, JAMF Software, the JAMF Software logo, the JAMF Software Server (JSS), and Self Service are trademarks of JAMF Software, LLC, registered in the United States and other countries.

All other product and service names mentioned are the trademarks of their respective companies.

JAMF Software would like to acknowledge Rich Trouton for contributing content to this technical paper.

Contents

Page 4	Introduction Target Audience What's in This Guide Important Concepts Additional Resources
Page 5	Overview
Page 6	Requirements
Page 7	Deploying the Recovery Keychain Creating a Recovery Keychain Removing the Private Key from the Recovery Keychain Creating a Recovery Keychain Package Uploading the Recovery Keychain Package (Optional) Uploading the enableFileVault.scpt Script Creating a Smart Group Deploying the Recovery Keychain
Page 17	Activating FileVault 2 Disk Encryption Activating FileVault 2 Disk Encryption with Self Service Activating FileVault 2 Disk Encryption Manually
Page 21	Reporting on FileVault 2 Encryption Status
Page 23	Accessing Encrypted Data Resetting an Account Password Using an Alternate Authorized Account Decrypting a Drive Using an Alternate Authorized Account Decrypting a Drive Using the Recovery Keychain

Introduction

Target Audience

This guide is designed for system administrators who plan to administer FileVault 2 on OS X v10.7 (Lion) with the Casper Suite.

What's in This Guide

This guide provides step-by-step instructions for configuring, activating, and reporting on FileVault 2 disk encryption with the Casper Suite. It also explains how to access encrypted data after FileVault 2 disk encryption is activated.

Important Concepts

Before using this guide, make sure you are familiar with the following Casper Suite-related concepts:

- Package and script management
- Deployment
- Advanced computer searches
- Smart computer groups

Additional Resources

For more information on applications, concepts, and processes related to the Casper Suite, see the *Casper Suite Administrator's Guide*, available at:

<http://jamfsoftware.com/resources/documentation>

For instructions on how to administer FileVault 2 on OS X v10.8, download the "Administering FileVault 2 on Mountain Lion with the Casper Suite" technical paper from:

http://www.jamfsoftware.com/libraries/pdf/white_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf

For more information on FileVault 2, see the following Apple Knowledge Base articles:

- "OS X Lion: About FileVault 2", available at:
<http://support.apple.com/kb/HT4790>
- "OS X Lion: Using FileVault 2 and Lion Recovery", available at:
<http://support.apple.com/kb/HT4811>
- "OS X Lion: FileVault 2 and Network Users", available at:
<http://support.apple.com/kb/HT4652>

Overview

The Casper Suite allows you to manage FileVault 2 disk encryption on OS X v10.7 computers by centralizing the packaging and distribution of settings that are required to activate disk encryption. After activating FileVault 2 disk encryption, you can report on FileVault 2 encryption status and access encrypted data.

Requirements

To administer FileVault 2 using the instructions in this guide, you need:

- The Casper Suite v8.3 or later running in your environment
- An administrator's computer with a version of OS X Lion v10.7.2 or later
- Client computers with a version of OS X Lion v10.7.2 or later
- A "Recovery HD" partition present on client computers
- Access to the JAMF Software Server (JSS)
- Casper Admin
- Composer
- (Optional) The `enableFileVault.scpt` script in the Casper Suite Resource Kit

You can download the Resource Kit from:

<http://www.jamfsoftware.com/downloads/ResourceKit.dmg>

Deploying the Recovery Keychain

Before activating FileVault 2 disk encryption on client computers, you need to deploy a recovery keychain. A recovery keychain contains a private key and a public key and can be used to access encrypted data after FileVault 2 disk encryption is activated.

Deploying the recovery keychain involves the following steps:

1. Create a recovery keychain.
2. Remove the private key from the recovery keychain.
3. Create a recovery keychain package.
4. Upload the recovery keychain package.
5. (Optional) Upload the `enableFileVault.scpt` script.
6. Create a smart group.
7. Deploy the recovery keychain using one of the following methods:
 - **Method 1: Making the Recovery Keychain Available in Self Service**
Create a policy to make the recovery keychain available in Self Service for users to install.
If you choose this method, users must have administrator privileges. You must also upload the `enableFileVault.scpt` script in addition to the recovery keychain package. This script will guide users through the process of activating FileVault 2 disk encryption.
 - **Method 2: Deploying the Recovery Keychain Automatically**
Create a policy to deploy the recovery keychain package.
If you choose this method, you will have to manually activate FileVault 2 disk encryption.

Creating a Recovery Keychain

1. On an administrator computer, open Terminal and execute the following command:

```
sudo security create-filevaultmaster-keychain /Library/Keychains/  
FileVaultMaster.keychain
```

2. Enter a master password when prompted.

A recovery keychain (`FileVaultMaster.keychain`) is created in the following location:
`/Library/Keychains/`

Note: If the computer is running OS X 10.7.2, a keychain certificate (`FileVaultMaster.cer`) is also created in `/Library/Keychains/`.

3. Copy the recovery keychain and save it in a secure location.
The recovery keychain will be used for data recovery in the future.

Removing the Private Key from the Recovery Keychain

For client computers to recognize the recovery keychain, you need to remove the private key.

To remove the private key from the recovery keychain:

1. Unlock the recovery keychain by opening Terminal and executing:

```
security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
```

2. Remove the private key.
 - a. Open the Keychain Access application and select the recovery keychain (FileVaultMaster.keychain) in the Keychains list in the sidebar.
 - b. Select the key called "FileVault Master Password Private Key," and then press the Delete key.
 - c. When prompted, click the **Delete** button and authenticate.
 - d. If the computer is running OS X 10.7.2, go to /Library/Keychains/ and delete the keychain certificate (FileVaultMaster.cer).

1. Re-lock the recovery keychain by executing:

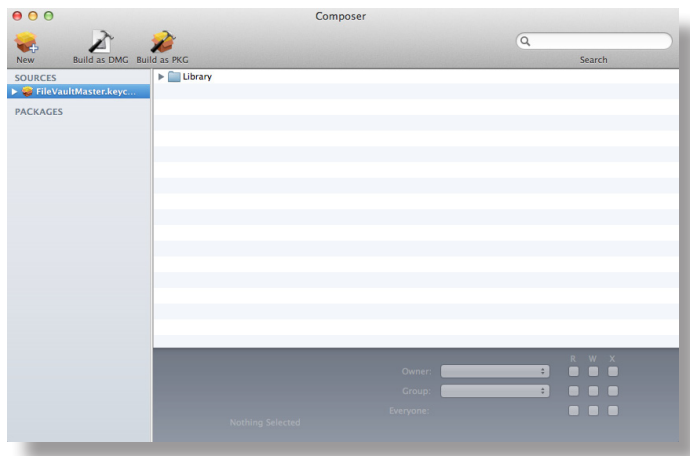
```
security lock-keychain /Library/Keychains/FileVaultMaster.keychain
```

Creating a Recovery Keychain Package

1. Open Composer and authenticate locally.
2. Locate the recovery keychain (FileVaultMaster.keychain), and then drag it to the sidebar in Composer.

The file will appear under the Sources heading.

3. Verify that Composer has obtained the appropriate source files for the package.



4. Select the recovery keychain package source from the Sources list in the sidebar, and then click **Build as DMG** or **Build as PKG**.
5. Select a location to save the package and click **Save**.

Uploading the Recovery Keychain Package

Upload the recovery keychain package to the JSS so you can deploy it with a policy.

To upload the recovery keychain package:

1. Open Casper Admin and log in using credentials for a JSS administrator account.
2. Locate the recovery keychain package, and then drag it to the Package pane in Casper Admin.
3. Double-click the recovery keychain package.
4. In the information pane that appears, click the **Info** tab and choose a category from the **Category** pop-up menu.
5. Click the **Options** tab and choose a priority from the **Priority** pop-up menu.
The recommended priority for the deployment package is "10". For more information on priorities, see the "Changing Package Attributes" section in the *Casper Suite Administrator's Guide*.
6. Configure additional settings as needed, and then click **OK**.
7. Save your changes and quit the application.

(Optional) Uploading the enableFileVault.scpt Script

If you plan to deploy the recovery keychain using a Self Service policy, upload the `enableFileVault.scpt` script to the JSS using Casper Admin.

To upload the enableFileVault.scpt script:

1. Open Casper Admin and log in using credentials for a JSS administrator account.
2. Locate the `enableFileVault.scpt` script, and then drag it to the Package pane in Casper Admin.

The `enableFileVault.scpt` script is located in the Casper Suite Resource Kit, available for download at <http://www.jamfsoftware.com/downloads/ResourceKit.dmg>.

3. Double-click the `enableFileVault.scpt` script.
4. In the information pane that appears, click the **Info** tab and choose a category from the **Category** pop-up menu.
5. Click the **Options** tab and choose a priority from the **Priority** pop-up menu.
The recommended priority for the script is "After". For more information on priorities, see the "Changing Script Attributes" section in the *Casper Suite Administrator's Guide*.
6. Configure additional settings as needed, and then click **OK**.
7. Save your changes and quit the application.

Creating a Smart Group

Create a smart group that can be used as the scope for deploying the recovery keychain package.

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Smart Computer Groups** link.
4. Click the **Create Smart Group** button in the toolbar.

- In the **Computer Group Name** field, enter a name for the group.

Edit Smart Computer Group:

ComputerGroup Name:

Send Email Notification on Change:

Field	Search Type	Criteria	-	+
Computer Information				+
Location Information				+
Hardware Information				+
Storage Information				+
OS Configuration Information				+
Software Information				+
Purchasing Information				+
Receipts Information				+
Extension Attributes Information				+

Cancel Save

- In the list of categories, click **Add (+)** across from **Storage Information**.
- Click **FileVault 2 Status** in the list of items.
- Choose **is not** from the pop-up menu.
- Click the **Ellipsis (...)** button, and then click **Boot Partition Encrypted** in the list of items.

Edit Smart Computer Group:

ComputerGroup Name:

Send Email Notification on Change:

Field	Search Type	Criteria	-	+
Computer Information				+
Location Information				+
Hardware Information				+
Storage Information				+
FileVault 2 Status	is not	Boot Partition Encrypted	⋮	+
OS Configuration Information				+
Software Information				+
Purchasing Information				+
Receipts Information				+
Extension Attributes Information				+

Cancel Save

10. Click **Add (+)** across from **OS Configuration Information**, and then click **Operating System** in the list of items.
11. Choose **like** from the pop-up menu, and then type "10.7" in the text field.
12. Click **Save**.

Deploying the Recovery Keychain

Deploy the recovery keychain using one of the following methods:

- **Method 1: Making the Recovery Keychain Available in Self Service**

Create a policy to make the recovery keychain available in Self Service for users to install.

If you choose this method, users must have administrator privileges. You must also upload the `enableFileVault.scpt` script in addition to the recovery keychain package. This script will guide users through the process of activating FileVault 2 disk encryption.

- **Method 2: Deploying the Recovery Keychain Automatically**

Create a policy to deploy the recovery keychain package.

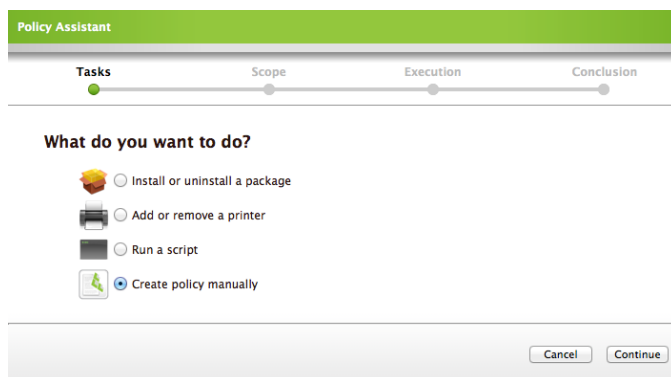
If you choose this method, you will have to manually activate FileVault 2 disk encryption.

Method 1: Making the Recovery Keychain Available in Self Service

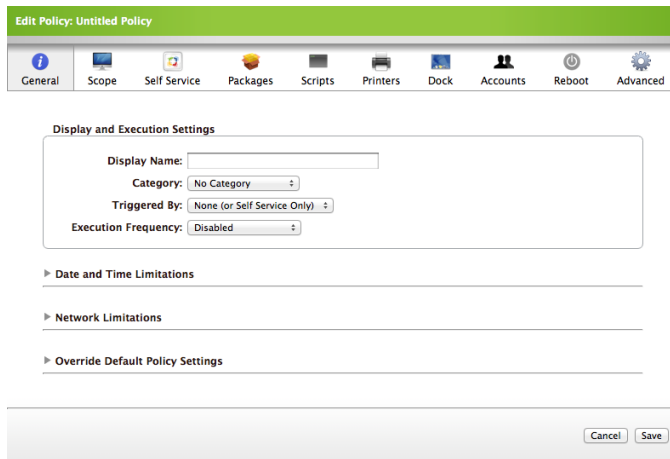
This section explains how to make the recovery keychain package and the `enableFileVault.scpt` script available in Self Service. Before using this method, make sure you have uploaded the `enableFileVault.scpt` script.

To make the recovery keychain available in Self Service:

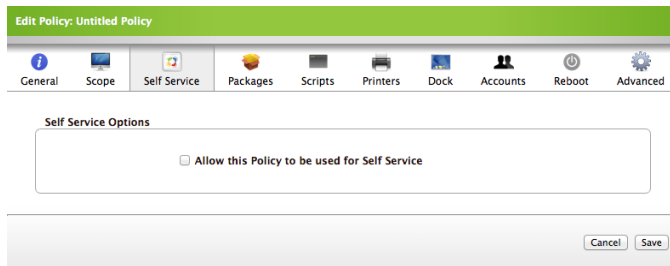
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select the **Create policy manually** option, and then click **Continue**.



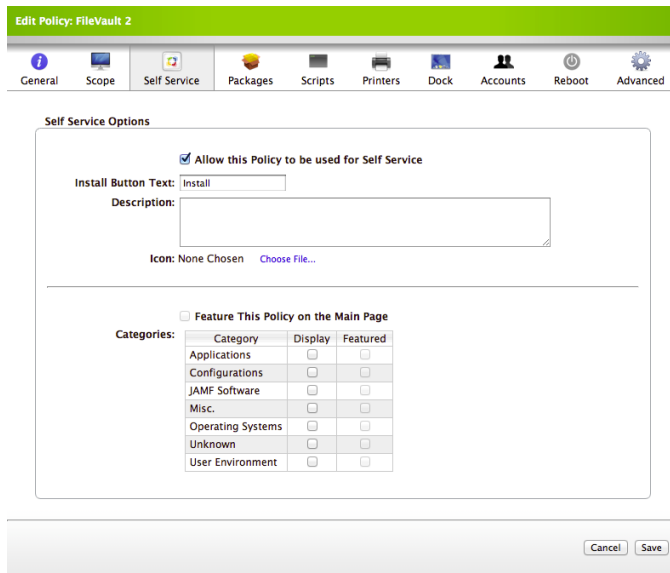
6. Enter a display name for the policy.



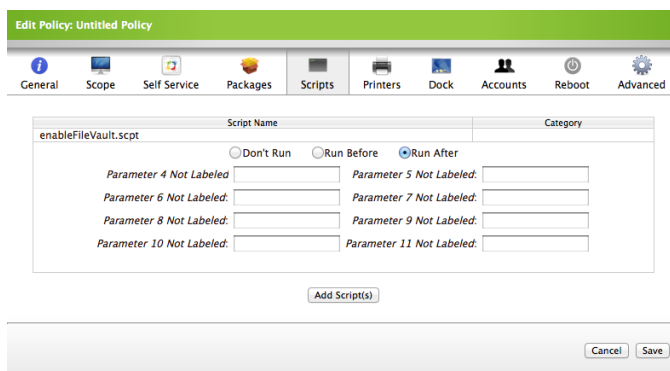
7. Assign the policy to a category using the **Category** pop-up menu.
8. Choose the "None (or Self Service Only)" trigger from the **Triggered By** pop-up menu.
9. Choose "Once per computer" from the **Execution Frequency** pop-up menu.
10. Click the **Scope** tab and assign a scope to the policy using the previously created smart computer group.
11. Click the **Self Service** tab and select the **Allow this Policy to be used for Self Service** checkbox.



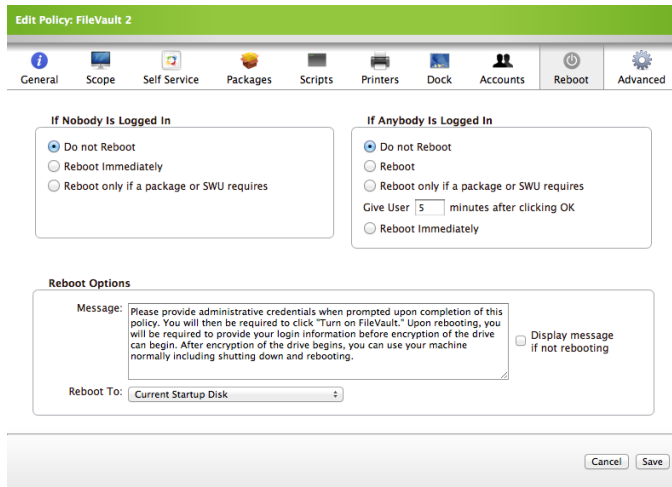
- Enter a description in the **Description** field if desired.



- To display an icon, click the **Choose File** link and upload an icon.
- If you uploaded an icon, select the **Feature this policy on the main page** checkbox to feature the policy on the main pane in Self Service.
- To display the policy in a category, select the **Display** checkbox across from the category. The category assigned on the General pane is selected by default.
- If you uploaded an icon, select the **Feature** checkbox across from the category to feature the policy in the category.
- Click the **Packages** tab, and then click the **Add Package** link.
- Locate the recovery keychain package and choose "Install" from the **Action** pop-up menu across from it.
- Click the **Add Package(s)** button.
- Click the **Scripts** tab and then click the **Add Script** link.
- Locate the `enableFileVault.scpt` script and select the **Run After** option.



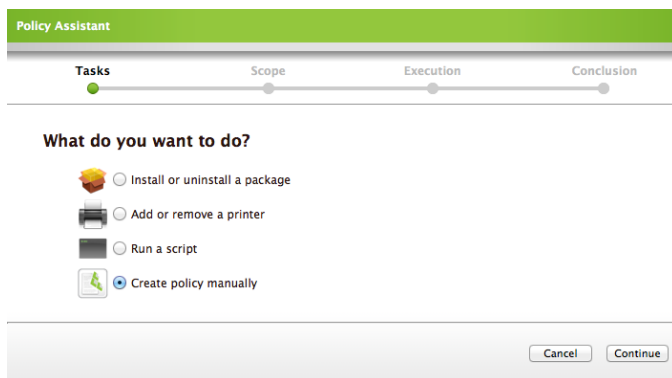
22. Click the **Add Script(s)** button.
23. Click the **Reboot** tab.
24. Select the **Do not Reboot** option in the “If Nobody Is Logged In” section of the pane.
25. Select the **Do not Reboot** option in the “If Anybody Is Logged In” section of the pane.
26. If desired, enter a message in the **Message** text field, and then select the **Display message if not rebooting** checkbox.



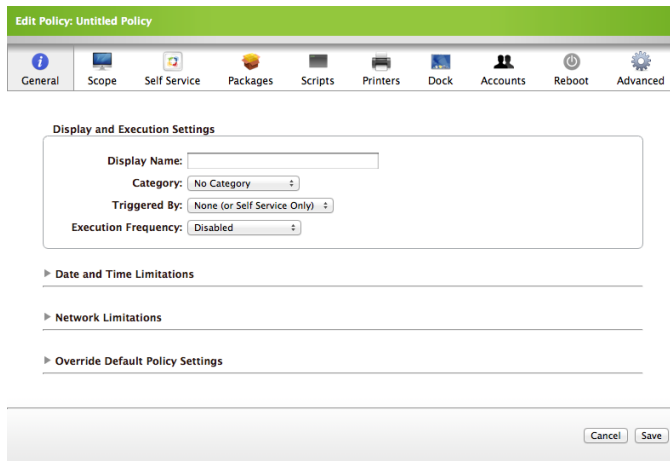
27. Click **Save**.

Method 2: Deploying the Recovery Keychain Automatically

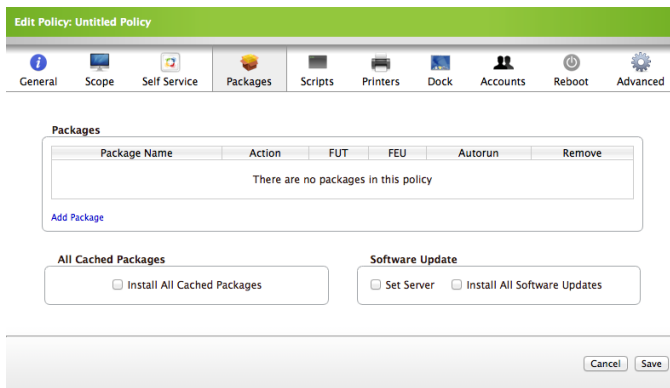
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select the **Create policy manually** option, and then click **Continue**.



6. Enter a display name for the policy.



7. Assign the policy to a category using the **Category** pop-up menu.
8. Choose the “startup” trigger from the **Triggered By** pop-up menu.
9. Choose “Once per computer” from the **Execution Frequency** pop-up menu.
10. Click the **Scope** tab and assign the previously created smart computer group to the scope.
11. Click the **Packages** tab, and then click the **Add Package** link.



12. Locate the recovery keychain package and choose “Install” from the **Action** pop-up menu across from it.
13. Click the **Add Package(s)** button.
14. Click **Save**.

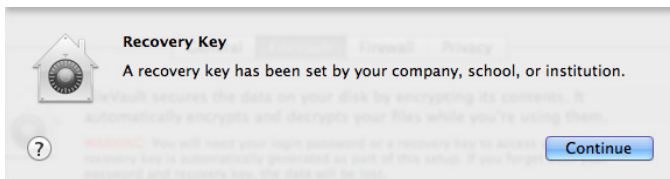
Computers in the scope execute the policy the next time they check in with the JSS.

Activating FileVault 2 Disk Encryption

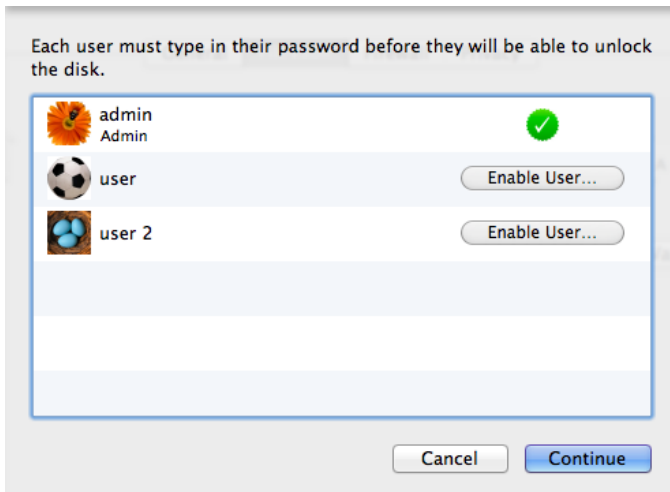
Once the recovery keychain is deployed, FileVault 2 disk encryption can be activated on client computers. If you made the recovery keychain available in Self Service, users can activate FileVault 2 disk encryption using Self Service. If you deployed the recovery keychain automatically, you need to manually activate FileVault 2 disk encryption on each client computer.

Activating FileVault 2 Disk Encryption with Self Service

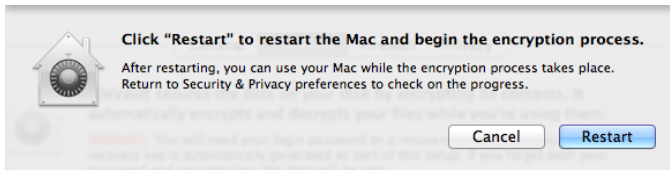
1. Open Self Service and locate the FileVault 2 policy that was previously created.
2. Click the **Install** button.
When the installation is complete, System Preferences launches.
3. Authenticate with credentials for a local administrator account when prompted.
4. Click **Turn On FileVault**.
5. Click **Continue**.



6. (Optional) Click the **Enable User** button across from your user name and enter your credentials when prompted.



7. Click **Continue**.
8. Click **Restart**.



9. The system restarts and prompts for authentication. Authenticate with credentials for a local administrator account.

Then, the system begins to encrypt the drive.



The computer can be used normally during encryption. To view the encryption status, open System Preferences and click **Security & Privacy**. Then, click the **FileVault** tab.

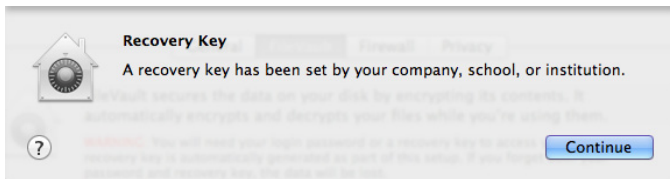
Activating FileVault 2 Disk Encryption Manually

1. Log in to the client computer with a local administrator's account.
2. Open System Preferences and click **Security & Privacy**.
3. Click the **FileVault** tab.

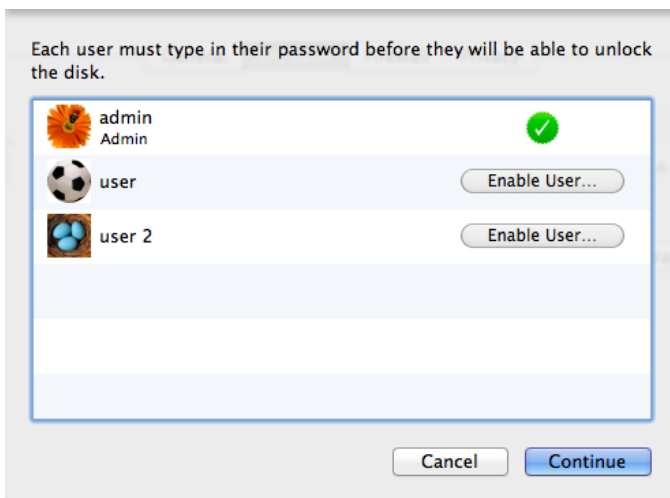
4. Click the **Lock** button in the bottom left corner to unlock the preferences.



5. Authenticate with credentials for a local administrator account when prompted.
6. Click the **Turn On FileVault** button.
7. Click **Continue**.



8. (Optional) Click **Enable User** and provide that user's credentials. Repeat this step until all additional accounts are added.



9. Click **Continue**.
10. Click **Restart**.



The system restarts and prompts for authentication. Authenticate with a local administrator's credentials.

Then, the system begins to encrypt the drive.



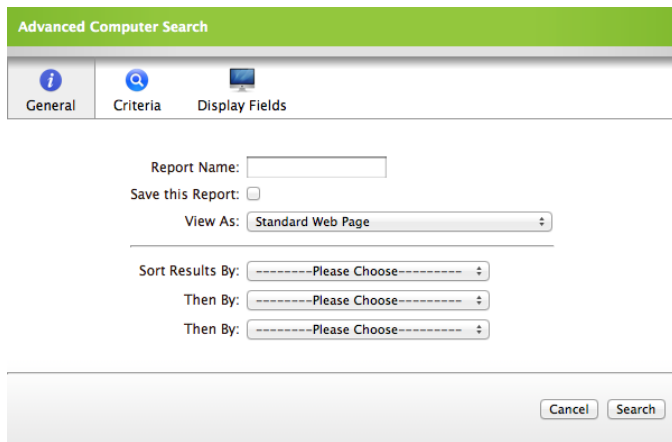
The computer can be used normally during encryption. To view the encryption status, open System Preferences and click **Security & Privacy**. Then, click the **FileVault** tab.

Reporting on FileVault 2 Encryption Status

After activating FileVault 2 disk encryption on client computers, you can use the Casper Suite to create a saved advanced search that tracks which computers have encrypted drives.

To create a saved advanced search to report on FileVault 2 Status:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Advanced Search** link.
4. Enter a name for the search in the **Report Name** field, and select the **Save this Report** checkbox.



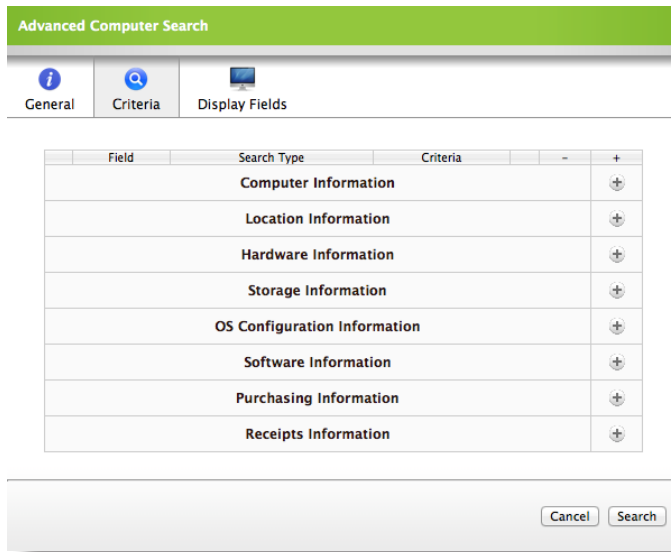
The screenshot shows the 'Advanced Computer Search' dialog box. It has a green header bar with the title 'Advanced Computer Search'. Below the header are three tabs: 'General' (selected), 'Criteria', and 'Display Fields'. The 'General' tab contains the following fields and controls:

- Report Name:** A text input field.
- Save this Report:** A checkbox.
- View As:** A dropdown menu currently set to 'Standard Web Page'.
- Sort Results By:** A dropdown menu with '-----Please Choose-----' selected.
- Then By:** A dropdown menu with '-----Please Choose-----' selected.
- Then By:** A second dropdown menu with '-----Please Choose-----' selected.

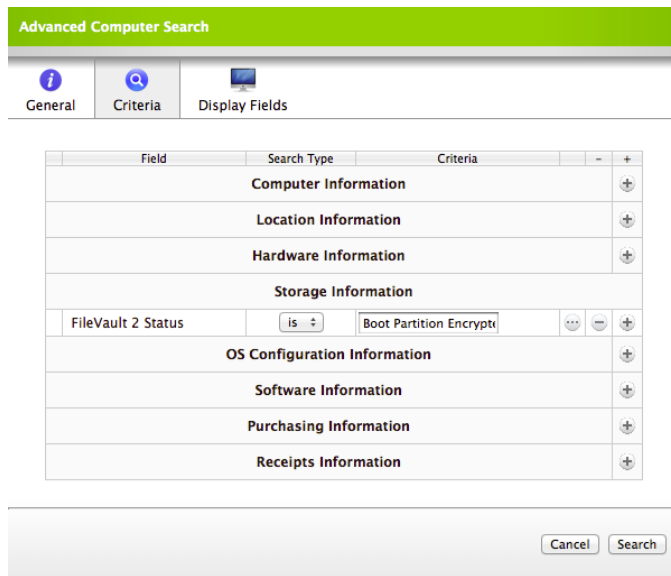
At the bottom right of the dialog are two buttons: 'Cancel' and 'Search'.

5. Click the **Criteria** tab.

- In the list of categories, click **Add (+)** across from **Storage Information**.



- Click **FileVault 2 Status** in the list of items.
- Choose "is" from the pop-up menu.
- Click the **Ellipsis (...)** button, and then click **Boot Partition Encrypted** in the list of items.
- Click **Add (+)** across from **OS Configuration Information**.



- Click **Operating System** in the list of items.
- Choose "like" from the pop-up menu and type "10.7" in the text field.
- Click **Search**.

Accessing Encrypted Data

FileVault 2 allows you to access and recover the data on a user's encrypted drive without the user's login credentials. The way you access encrypted data depends on the number of accounts that are authorized to unlock the encrypted drive.

If more than one account is authorized to unlock the drive, there are two ways to access encrypted data:

- Reset the password for the user's account using an alternate authorized account. This allows you to recover data by simply logging in to the user's account.
- Decrypt the drive using an alternate authorized account. This requires you to use the command line to recover data.

If only one account is authorized to unlock the encrypted drive, you must decrypt the drive using the recovery keychain. Then, you can:

- Reset the account password using the Reset Password utility and recover data by simply logging in to the user's account.
- Recover data using the command line.

Resetting an Account Password Using an Alternate Authorized Account

You can use this method to access encrypted data if more than one account is authorized to unlock the drive.

To reset an account password using an alternate authorized account:

1. Restart the computer with the encrypted drive.
2. When prompted with the FileVault pre-boot screen, enter credentials for a secondary authorized account.
3. Ensure that you are logged in as an administrator.
4. Open System Preferences and click **Users & Groups**.
5. If needed, click the lock and enter your password to make changes.
6. Select the primary account in the sidebar and click the **Reset Password** button.

7. Enter a new password, and then enter it again to verify it. Then, click the **Reset Password** button.

You can now recover data by restarting the computer and entering credentials for the user's account when prompted with the FileVault pre-boot screen.

Decrypting a Drive Using an Alternate Authorized Account

You can use this method to access encrypted data if more than one account is authorized to unlock the drive.

To decrypt a drive using an alternate authorized account:

1. Restart the computer with the encrypted drive while pressing **Command + R**. This boots the computer to the "Recovery HD" partition.
2. Open Disk Utility.
3. From the menu bar, choose **File > Unlock "Macintosh HD"** or **File > Turn Off Encryption**.
4. Enter the password for the alternate authorized account.

The system begins to decrypt the drive. The computer can be used normally during decryption.

To view the decryption status, open System Preferences and click **Security & Privacy**. Then, click the **FileVault** tab.

After the drive is decrypted, you can recover data using the command line.

Decrypting a Drive Using the Recovery Keychain

Use this method to access encrypted data if only one account is authorized to unlock the drive.

To decrypt a drive using the recovery keychain:

1. Restart the computer with the encrypted drive while pressing **Command + R**. This boots the computer to the "Recovery HD" partition.
2. Open Terminal.
3. Unlock the recovery keychain by executing:

```
security unlock-keychain <path to the secure copy of the  
FileVaultMaster.keychain file>
```

4. Locate the UUID of the encrypted disk by executing:

```
diskutil cs list
```


5. Unlock the encrypted drive with the UUID and recovery keychain by executing:

```
diskutil cs unlockVolume <UUID> -recoveryKeychain <path to the  
secure copy of the FileVaultMaster.keychain file>
```

6. Turn off encryption by executing the following command:

```
diskutil cs revert <UUID> -recoveryKeychain <path to the secure copy  
of the FileVaultMaster.keychain file>
```

After the drive is decrypted, you can reset the account password using the Reset Password utility and recover data by simply logging in to the user's account. Or, you can recover data using the command line.

To reset an account password using the Reset Password utility:

1. Restart the computer with the encrypted drive while pressing **Command + R**. This boots the computer to the "Recovery HD" partition.
2. Open Terminal and launch the Reset Password utility by executing:

```
resetpassword
```

3. Use the Reset Password utility to reset the account's password.
4. Restart the computer and log in using the new password.