Administering FileVault 2 on OS X Mountain Lion with the Casper Suite

Technical Paper
Casper Suite v8.6-8.7
14 August 2013

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

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

Contents

Introduction

Target Audience

This guide is intended for system administrators who plan to administer FileVault 2 on OS X v10.8 (Mountain Lion) with the Casper Suite.

What's in This Guide

This guide provides step-by-step instructions for administering FileVault 2 on OS X v10.8 with the Casper Suite.

Important Concepts

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

- Deployment
- Advanced computer searches

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 v10.7, download the "Administering FileVault 2 on Lion with the Casper Suite" technical paper from:

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

Overview

The Casper Suite allows you to manage FileVault 2 disk encryption on OS X v10.8 computers by creating and deploying a disk encryption configuration using the JAMF Software Server (JSS). After activating FileVault 2 disk encryption, you can view the FileVault 2 recovery key, and report on disk encryption progress and on enabled FileVault 2 users.

This paper provides a complete workflow for administering FileVault 2, which involves the following steps:

1. Choose a recovery key.
2. Create and export an institutional recovery key (for institutional recovery keys only).
3. Create a disk encryption configuration.
4. Deploy the disk encryption configuration.
5. Report on FileVault 2 disk encryption.
6. Access encrypted data.

Requirements

Administering FileVault 2 on OS X v10.8 requires:

- The Casper Suite v8.6-8.7 running in your environment
- An administrator's computer with OS X v10.8
- Client computers with OS X v10.8
- A "Recovery HD" partition present on client computers
- Access to the JAMF Software Server (JSS)
- A JSS user account with the following privileges:
    - View Disk Encryption Recovery Key
    - Manage Disk Encryption
    - Enable Disk Encryption Configuration Remotely
    - Manage Disk Encryption Institutional Key

Note: The "Enable Disk Encryption Configuration Remotely" privilege is only required if you plan to deploy the disk encryption configuration using Casper Remote. The "Manage Disk Encryption Institutional Key" privilege is only required if you plan to use an institutional key in your disk encryption configuration.

Choosing a Recovery Key

The first step to administering FileVault 2 disk encryption is to choose the type of recovery key that you want to use. Recovery keys allow you to access data on encrypted drives after disk encryption is activated.

There are two types of recovery keys:

- **Individual**—Uses a unique recovery key for each client computer. Individual recovery keys are created and stored in the JSS when the encryption takes place.
- **Institutional**—Uses a single recovery key that is shared by client computers. Institutional recovery keys must be created with Keychain Access, and then uploaded to the JSS for storage.

You can also choose to use both recovery keys together in the JSS.

If you plan to use an institutional recovery key, you must first create the institutional recovery key using Keychain Access. For instructions, see "Creating and Exporting an Institutional Recovery Key".

Creating and Exporting an Institutional Recovery Key

To use an institutional recovery key, you must first create and export a recovery key using Keychain Access.

You can export the recovery key with or without the private key. Exporting with the private key allows you to store it in the JSS. If you export without the private key, you must store it in a secure location so you can access it later if you need to.

To create an institutional recovery key and export it with the private key:

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

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

2. Enter a password for the new keychain when prompted.

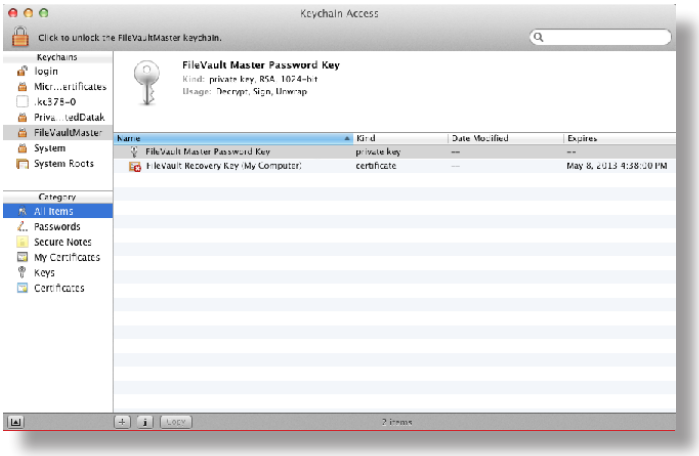
   A keychain (`FileVaultMaster.keychain`) is created in the following location:

   `/Library/Keychains/`

3. Unlock the keychain by opening Terminal and executing:

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

4. Create a copy of the keychain and save it in a secure location.
5. Open Keychain Access.
6. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading in the sidebar.
7. Verify that a private key is associated with it.



8. Select the certificate and the private key.
9. From the menu bar, choose **File** > **Export Items** and save the items as a .p12 file.
   The .p12 file is a bundle that contains both the FileVault Recovery Key and the private key.
10. Create and verify a password to secure the file, and then click **OK**.
    You will need to enter this password when you create a disk encryption configuration in the JSS.

11. Quit Keychain Access.

The FileVault Recovery Key and the private key are saved as a .p12 file in the location you specified.

To create an institutional recovery key and export it without the private key:

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

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

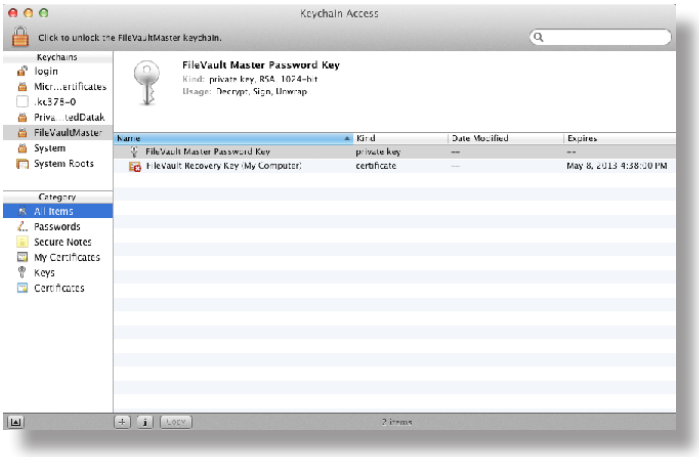
2. Enter a password for the new keychain when prompted.
   A keychain (`FileVaultMaster.keychain`) is created in the following location:
   `/Library/Keychains/`
3. Unlock the keychain by opening Terminal and executing:

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

4. Open Keychain Access.
5. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading in the sidebar.

6. Select the certificate.

   Do not select the private key that is associated with the certificate.



7. From the menu bar, choose **File** > **Export Items** and save the recovery key as a .pem file or .cer file. This is the file you upload to the JSS.

8. Quit Keychain Access.

9. Store the keychain (`FileVaultMaster.keychain`) in a secure location so you can use it to decrypt a drive at a later time.

   The FileVault Recovery Key is saved as a .cer file or a .pem file in the location you specified.

Creating a Disk Encryption Configuration

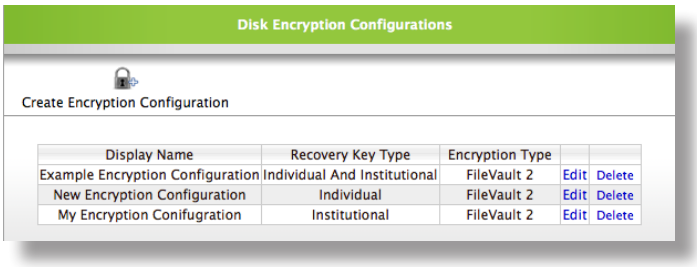
The JSS allows you to create a disk encryption configuration that you can deploy to activate FileVault 2.

Disk encryption configurations allow you to set the following information:

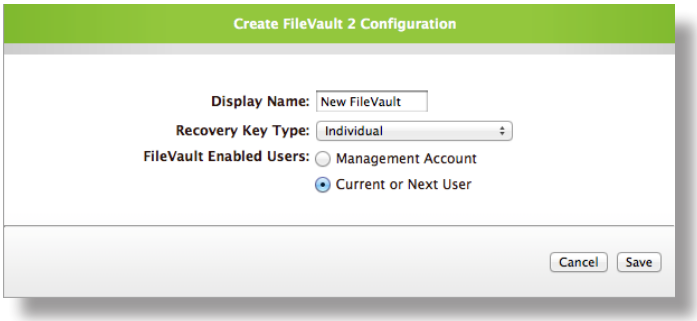
- The type of recovery key to use for encrypted drives.
- The user that will be the enabled FileVault 2 user.

To create a disk encryption configuration:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Disk Encryption Configurations** link.
4. Click the **Create Encryption Configuration** button.



5. Enter a name for the disk encryption configuration in the **Display Name** field.



6. Choose a type of recovery key from the **Recovery Key Type** pop-up menu.

7. If you choose to use an institutional recovery key or an individual and institutional recovery key, upload the recovery key file to the JSS:
   a. Click the **Upload** button.
   b. Click the **Choose File** button and select the recovery key file.

      The recovery key must be a .p12, .cer, or .pem file.
   c. Click the **Upload Selected File** button.

      If you are uploading a .p12 file, you are prompted to enter your password. Enter the password that you created when you exported the recovery key from Keychain Access.
   d. Click the **Save** button.

8. Choose the user that you want to be the enabled FileVault 2 user.
   - **Management Account**—Makes the management account on the computer the enabled FileVault 2 user.
   - **Current or Next User**—Makes the user that is logged into the computer when the encryption takes place the enabled FIleVault 2 user. If no user is logged in, the next user to log in becomes the enabled FileVault 2 user.
9. Click the **Save** button.

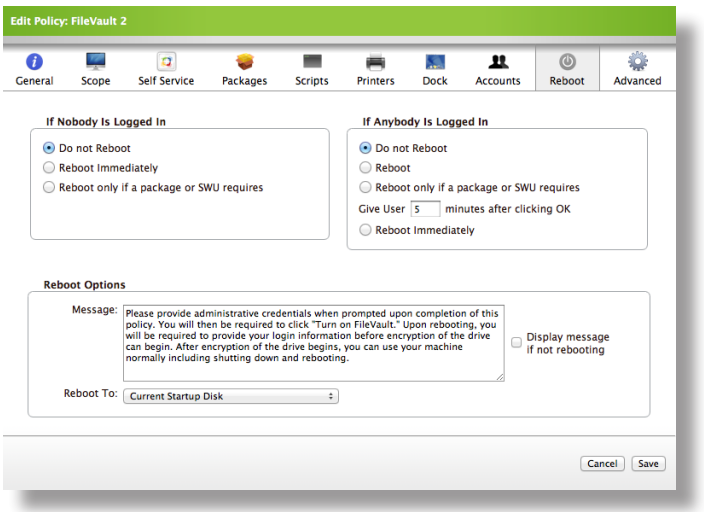
Deploying the Disk Encryption Configuration

To activate FileVault 2 disk encryption on client computers, deploy the disk encryption configuration that you created in the previous section using a policy or Casper Remote.

To deploy a disk encryption configuration using a policy:

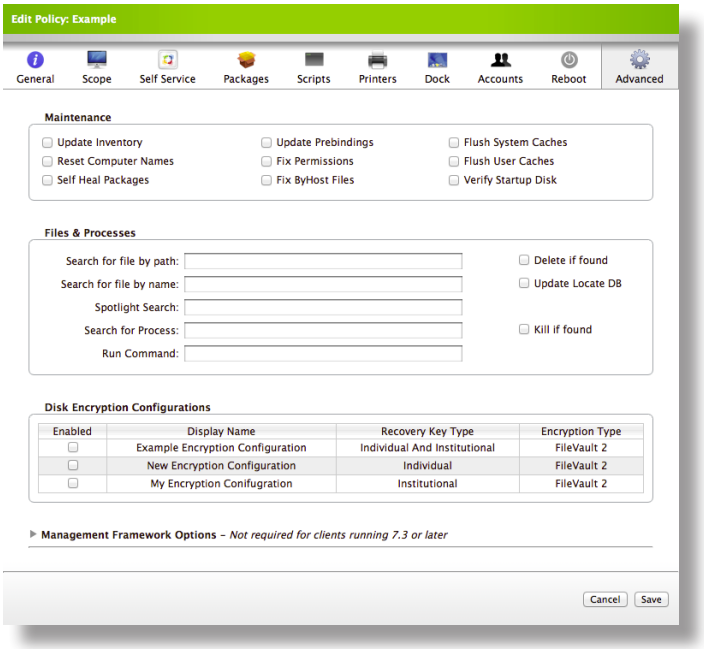
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select the **Create policy manually** option, and then click **Continue**.
6. Enter a display name for the policy.
7. Assign the policy to a category using the **Category** pop-up menu.
8. Choose a 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 computers or user groups to the scope.
11. (Optional) If you enabled the management account when you created the disk encryption configuration, click the **Reboot** tab and configure the desired reboot options.

    FileVault 2 disk encryption will not be activated until the next time computers in the scope are restarted.



12. Click the **Advanced** tab.

13. In the Disk Encryption Configurations section, select the checkbox in the **Enabled** column for the disk encryption configuration you want to deploy.



14. Click **Save**.

Clients execute the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

If you deployed a disk encryption configuration that is configured to use the management account as the enabled FileVault 2 user, the disk encryption is activated the next time computers are restarted.

If you deployed a disk encryption configuration that is configured to use the current or next user as the enabled FileVault 2 user, the disk encryption is activated next time users log out or computers are restarted by users.

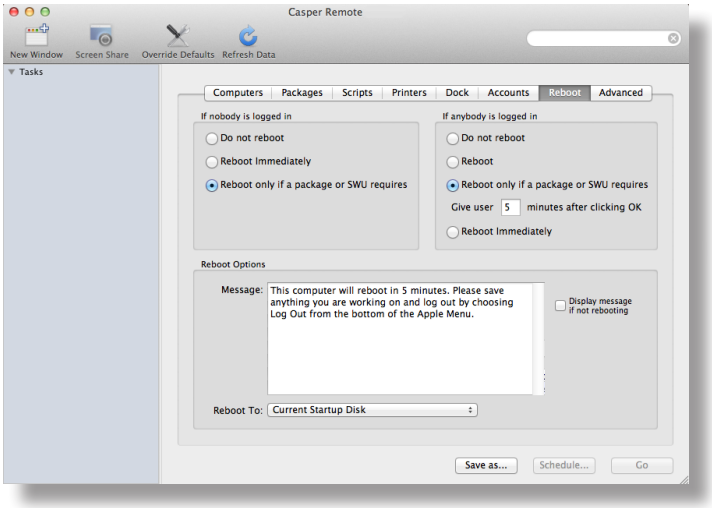
To deploy a disk encryption configuration using Casper Remote:

1. Open Casper Remote.

2. In the **Computers** list, locate the computers you want to deploy the disk encryption configuration to and select the checkbox next to each one.

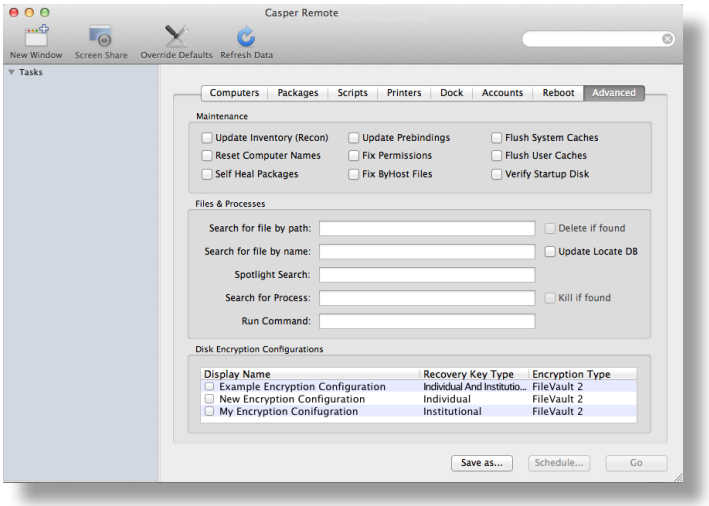
3. (Optional) If you enabled the management account when you created the disk encryption configuration, click the **Reboot** tab and configure the desired reboot options.

   FileVault 2 disk encryption will not be activated until the next time computers in the scope are restarted.



4. Click the **Advanced** tab.

5. In the list of Disk Encryption Configurations, select the checkbox next to the disk encryption configuration that you want to deploy.



6. Click **Go**.

   If you deployed a disk encryption configuration that is configured to use the management account as the enabled FileVault 2 user, the disk encryption is activated the next time computers are restarted.

   If you deployed a disk encryption configuration that is configured to use the current or next user as the enabled FileVault 2 user, the disk encryption is activated next time users log out or computers are restarted by users.

Reporting on FileVault 2

After activating FileVault 2, you can use the JSS to create and save an advanced search to report on computers that have FIleVault 2 disk encryption. You can use this search to view the disk encryption progress and the recovery keys for computers that have FileVault 2-encyrpted drives.

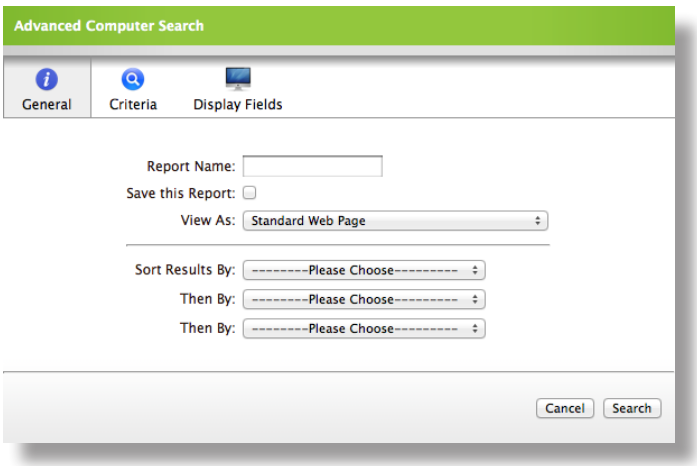
You can also create an advanced search to view the enabled FileVault user on a computer.

Creating and Saving an Advanced Search for FileVault 2 Disk Encryption

First create and save an advanced search that allows you to report on FileVault 2 disk encryption. This report returns all OS X v10.8 computers that have FileVault 2-encrypted drives.

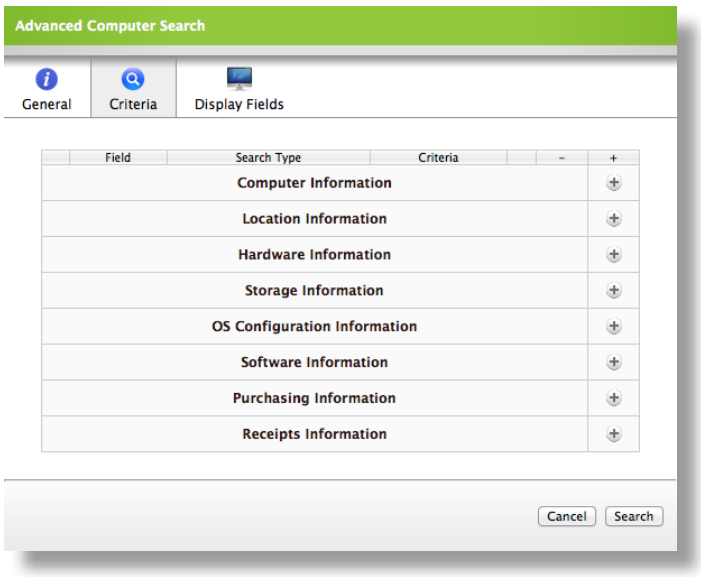
To create and save an advanced search for FileVault 2 disk encryption:

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.
5. Select the **Save this Report** checkbox.

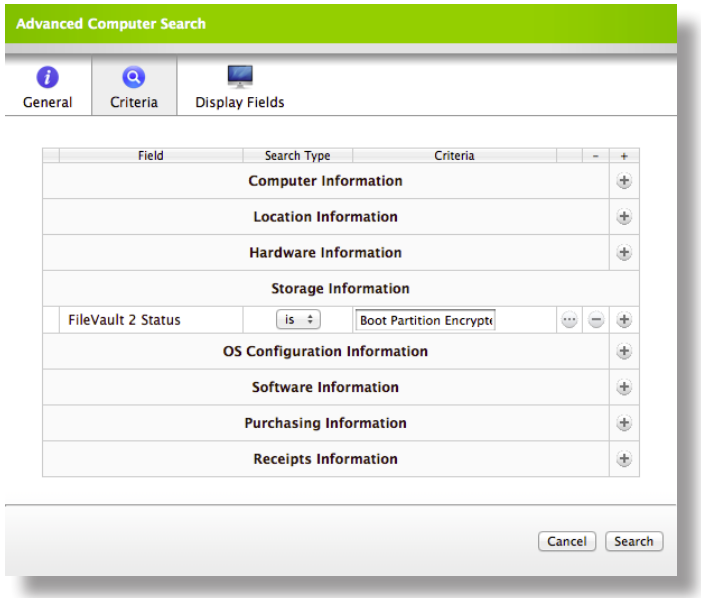


6. Click the **Criteria** tab.

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



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



12. Click **Operating System** in the list of items.
13. Choose "like" from the pop-up menu and type "10.8" in the text field.
14. Click **Search**.

Viewing Disk Encryption Progress

You can use the advanced search that you created in the "Creating and Saving an Advanced Search for FileVault 2 Disk Encryption" section to view the disk encryption progress for a FileVault 2-enabled computer.

To view the disk encryption progress:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. In the list of Saved Computer Searches, click the saved search that you created in the "Creating and Saving an Advanced Search for FileVault 2 Disk Encryption" section.
4. Locate the computer that you want to view the disk encryption progress for, and click the **Details** link across from it.
5. Click **Storage** in the list of categories.

   The disk encryption progress is displayed next to the **FileVault 2 Percentage** field.

Viewing Recovery Keys

You can use the advanced search that you created in the "Creating and Saving an Advanced Search for FileVault 2 Disk Encryption" section to view the recovery key for a FileVault 2-enabed computer.

To view a recovery key:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. In the list of Saved Computer Searches, click the saved search that you created in the "Creating and Saving an Advanced Search for FileVault 2 Disk Enryption" section.
4. Locate the client computer that you want to view the recovery key for, and click the **Details** link across from it.
5. Click **Storage** in the list of categories.
6. Click the  icon next to the **FileVault 2 Recovery Key** field.
   - If the recovery key is an "Individual" or an "Insitutional" recovery key, click the **Download** link to download the recovery key.
   - If the recovery key is an "Individual And Institutional" recovery key, the individual recovery key is displayed next to the **FileVault 2 Recovery Key** field.

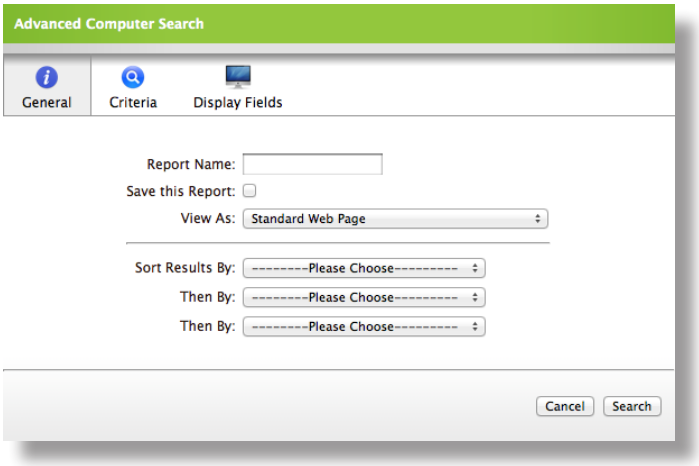
     You can view the institutional recovery key by clicking the **Download** link.

Reporting on Enabled FileVault 2 Users

You can create and save an advanced search to view the enabled FileVault 2 users on a computer.

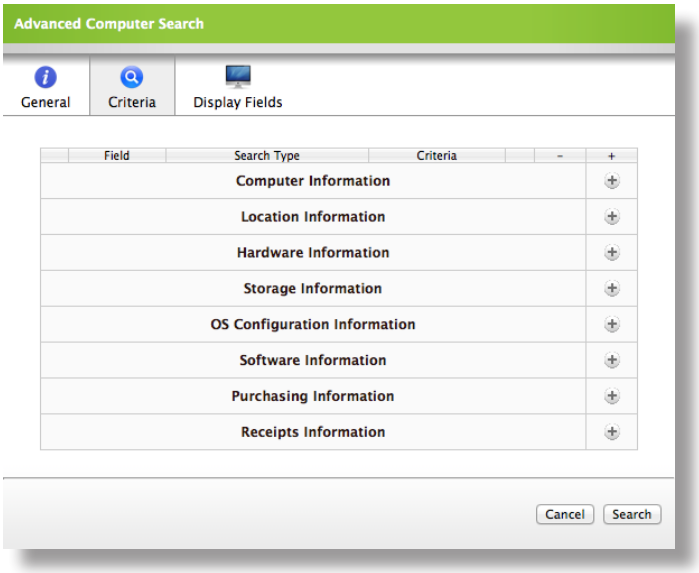
To report on enabled FileVault 2 users:

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.
5. Select the **Save this Report** checkbox.



6. Click the **Criteria** tab.
7. In the list of categories, click **Add (+)** across from **OS Configuration Information**.
8. Click **Operating System** in the list of items.
9. Choose "like" from the pop-up menu and type "10.8" in the text field.

10. In the list of categories, click **Add** (+) across from **OS Configuration Information.**



11. Click **FileVault Status** in the list of items.
12. Choose "is" from the pop-up menu.
13. Click the **Ellipsis (...)** button, and then click **All Accounts** in the list of items.
14. 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 key. 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 Key

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

Note: If you used an institutional recovery key with the private key, and you no longer have the keychain, you need to download the `RecoveryKey.p12` file from the JSS and covert it to a .keychain file. For instructions, see the following Knowledge Base article:

https://jamfnation.jamfsoftware.com/article.html?id=304

To decrypt a drive using the recovery key:

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 key by executing:

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

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

```
diskutil cs list
```

5. Unlock the encrypted drive with the Logical Volume UUID and recovery key 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.