

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

Technical Paper
Casper Suite v9.0 or Later
7 January 2015



 JAMF Software, LLC
© 2015 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

Composer, the Composer logo, JAMF Software, Recon, and the Recon logo are trademarks of JAMF Software, LLC, registered in the U.S. and other countries.

FileVault, the FileVault logo, Keychain Access, and Mac OS X are registered trademarks of Apple Inc., 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 What's in This Guide Important Concepts Additional Resources
Page 5	Overview
Page 6	Requirements
Page 7	Choosing a Recovery Key
Page 8	Creating and Exporting an Institutional Recovery Key Creating and Exporting an Institutional Recovery Key with the Private Key Creating and Exporting an Institutional Recovery Key Without the Private Key
Page 11	Creating a Disk Encryption Configuration
Page 13	Deploying the Disk Encryption Configuration
Page 16	Reporting on FileVault 2 Reporting on FileVault 2-Encrypted Drives Viewing Disk Encryption Progress Viewing FileVault 2 Recovery Keys Reporting on Enabled FileVault 2 Users
Page 20	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 Key

Introduction

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

Administrators using this guide should be familiar with the following Casper Suite-related concepts:

- Deployment
- Advanced computer searches

Additional Resources

For more information on related topics, see the *Casper Suite Administrator's Guide*, available at: <http://jamfsoftware.com/product-documentation/administrators-guides>

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 computers requires:

- The JSS v9.0 or later
- An administrator's computer with OS X v10.8
- Target computers with OS X v10.8 and a "Recovery HD" partition

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 to recover encrypted data.

There are two types of recovery keys:

- **Individual (also known as “Personal”)**—Uses a unique recovery key for each computer. Individual recovery keys are created and stored in the JSS when the encryption takes place.
- **Institutional**—Uses a shared recovery key. This requires you to create the recovery key with Keychain Access and upload to the JSS for storage.

You can also choose to use both recovery keys (individual and institutional) 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 when needed.

Creating and Exporting an Institutional Recovery Key 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
```

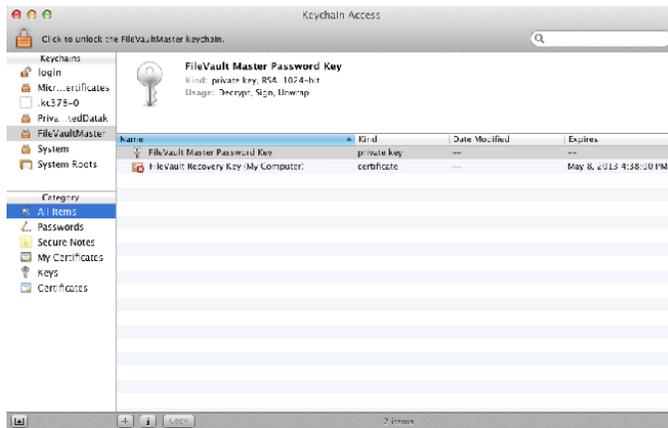
2. Enter a password for the new keychain when prompted.
A keychain (FileVaultMaster . keychain) is created in the following location:
/Library/Keychains/

3. Unlock the keychain by opening Terminal and executing:

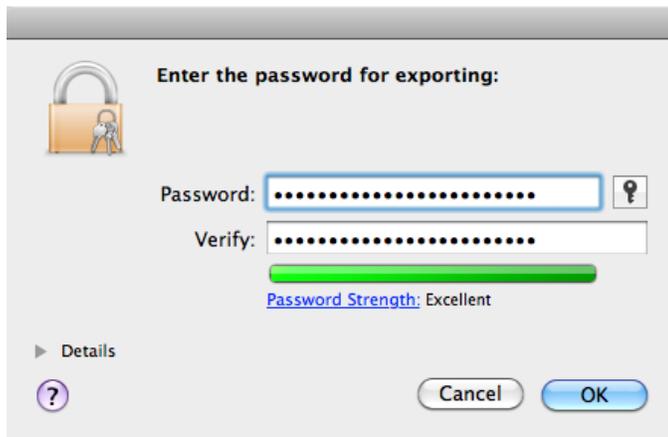
```
security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
```

4. Make a backup 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.

7. Verify that a private key is associated with the certificate.



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 be prompted enter this password when uploading the recovery key to 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.

Creating and Exporting an Institutional Recovery Key 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
```

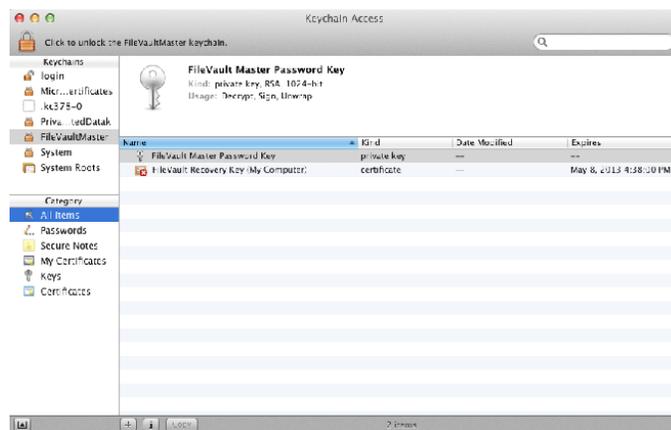
2. Enter a password for the new keychain when prompted.
A keychain (FileVaultMaster.keychain) is created in the following location:
/Library/Keychains/

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.
6. Select the certificate.

Do not select the private key 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. You will need to upload this file to the JSS when creating the disk encryption configuration.
8. Quit Keychain Access.
9. Store the keychain (FileVaultMaster.keychain) in a secure location so you can use it to access encrypted data at a later time.

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

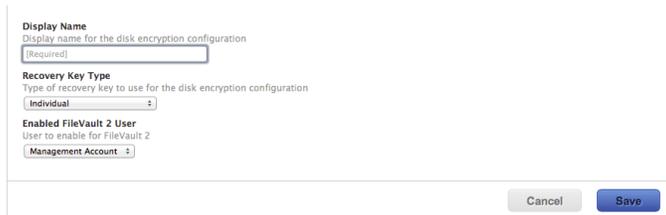
Creating a Disk Encryption Configuration

Creating a disk encryption configuration in the JSS is the first step to activating FileVault 2 on OS X v10.8 computers.

Disk encryption configurations allow you to configure the following information:

- The type of recovery key to use for recovering encrypted data
- The user for which to enable FileVault 2

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
On a smartphone, this option is in the pop-up menu.
4. In the “Computer Management” section, click **Disk Encryption Configurations** .
5. Click **New** .
6. Enter a name for the disk encryption configuration in the **Display Name** field.



Display Name
Display name for the disk encryption configuration
(Required)

Recovery Key Type
Type of recovery key to use for the disk encryption configuration
Individual

Enabled FileVault 2 User
User to enable for FileVault 2
Management Account

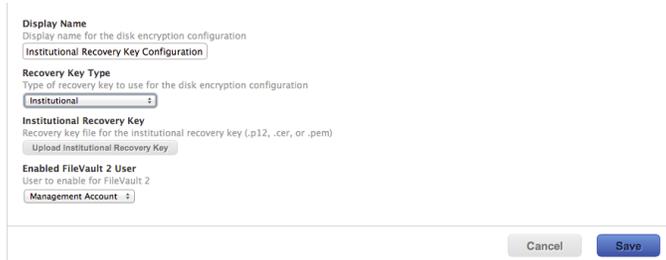
Cancel Save

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

8. If you chose an “Institutional” or “Individual and Institutional” recovery key, click **Upload Institutional Recovery Key** and upload the recovery key to the JSS.

The recovery key must be a .p12, .cer, or .pem file.

If you upload a .p12 file, you are prompted to enter the password that you created when exporting the key from Keychain Access.



The screenshot shows a dialog box titled "Institutional Recovery Key Configuration". It contains the following fields and options:

- Display Name:** A text field containing "Institutional Recovery Key Configuration".
- Recovery Key Type:** A dropdown menu with "Institutional" selected.
- Institutional Recovery Key:** A text field with a button labeled "Upload Institutional Recovery Key" next to it.
- Enabled FileVault 2 User:** A dropdown menu with "Management Account" selected.

At the bottom right of the dialog are "Cancel" and "Save" buttons.

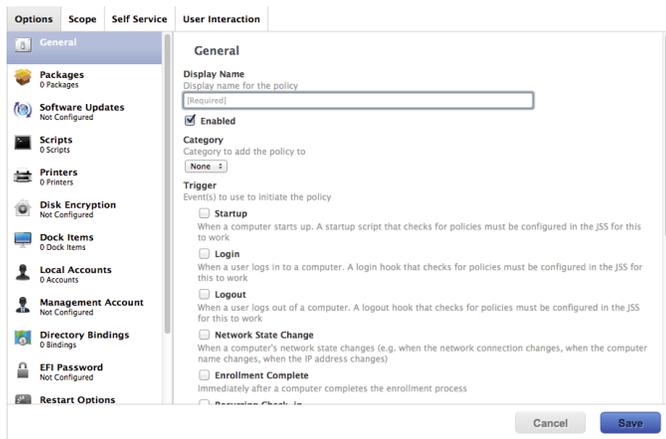
9. Choose the user for which to enable FileVault 2:
 - **Management Account**—Makes the management account on the computer the enabled FileVault 2 user.
 - **Current or Next User**—Makes the user that is logged in to the computer when the encryption takes place the enabled FileVault 2 user. If no user is logged in, the next user to log in becomes the enabled FileVault 2 user.
10. Click **Save**.

Deploying the Disk Encryption Configuration

After creating a disk encryption configuration, use a policy to deploy it to activate FileVault 2.

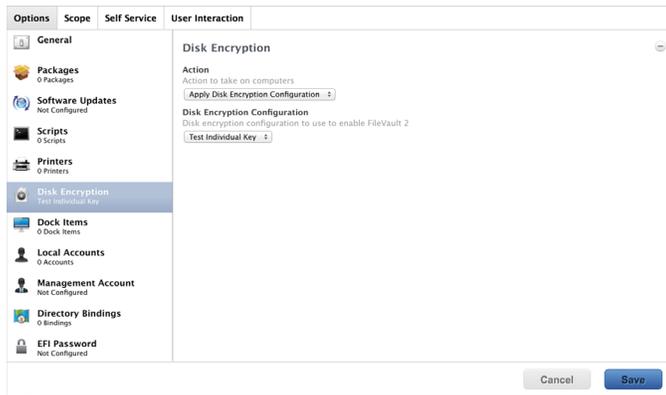
The event that activates FileVault 2 depends on the enabled FileVault 2 user specified in the disk encryption configuration. If the enabled user is “Management Account,” FileVault 2 is activated on a computer the next time the computer restarts. If the enabled user is “Current or Next User,” FileVault 2 is activated on a computer the next time the current user logs out or the computer restarts.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
On a smartphone, this option is in the pop-up menu.
4. Click **New**  .
5. In the General payload, enter a display name for the policy. For example, “FileVault 2 Disk Encryption”.



6. Select a trigger.
7. Choose “Once per computer” from the **Execution Frequency** pop-up menu.
8. Select the Disk Encryption payload and click **Configure**.

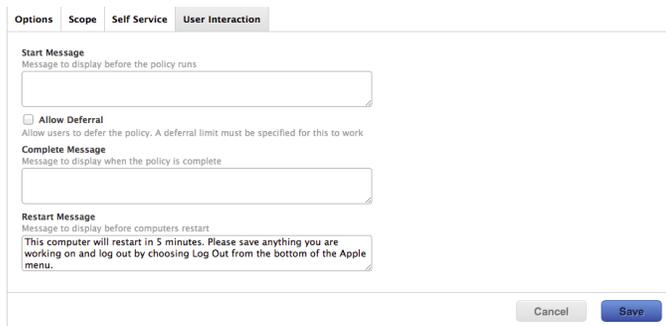
9. Choose the disk encryption configuration from the **Disk Encryption Configuration** pop-up menu.



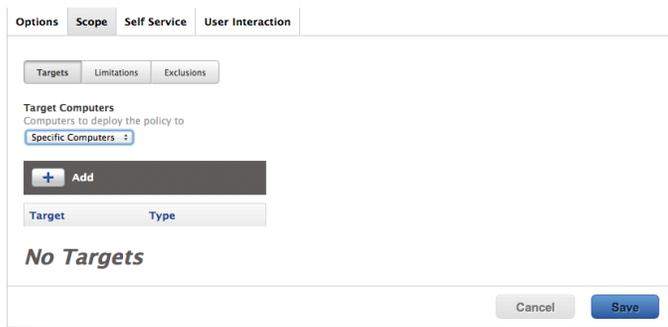
10. If “Management Account” is selected as the enabled FileVault 2 user in the disk encryption configuration, do the following:
- Click the Restart Options payload and configure restart settings for the computer.
 - (Optional) If you are using the Casper Suite v9.63 or later, select **Perform authenticated restart on computers with FileVault 2 enabled** to allow computers with OS X v10.8.2 or later that are FileVault 2 enabled to be restarted without requiring an unlock the next time the computer starts up.

For this to work on computers with FileVault 2 activated, the enabled FileVault 2 user must log in after the policy runs for the first time and the computer has restarted.

- (Optional) Click the **User Interaction** tab and customize the restart message displayed to users.



11. Click the **Scope** tab and configure the scope of the policy.



12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Reporting on FileVault 2

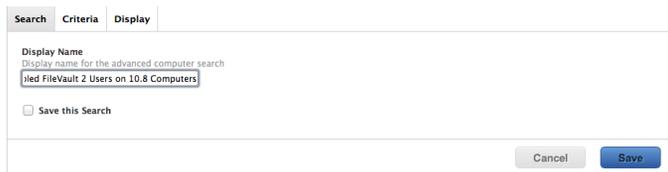
After activating FileVault 2, you can use the JSS to create and save an advanced computer search to report on computers that have FileVault 2-encrypted drives. You can use this search to view the disk encryption progress and the recovery keys for each encryption.

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

Reporting on FileVault 2-Encrypted Drives

First, create and save an advanced computer search that returns all OS X v10.8 computers with FileVault 2-encrypted drives.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. Use the Search pane to enter a display name for the search.
6. Select the **Save this Search** checkbox.



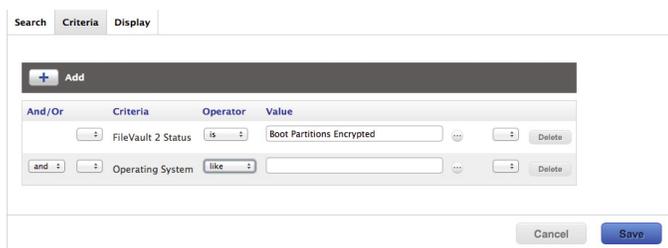
The screenshot shows a dialog box with three tabs: 'Search', 'Criteria', and 'Display'. The 'Search' tab is active. Below the tabs, there is a 'Display Name' label and a text input field containing 'FileVault 2 Users on 10.8 Computers'. Below the input field is a checkbox labeled 'Save this Search' which is checked. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

7. Click the **Criteria** tab.
8. Click **Add** .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault 2 Status".
When the "FileVault 2 Status" criteria is displayed, make sure the operator is set to "Is".

10. Click **Browse**  , and then click **Choose** for “Boot Partitions Encrypted”.



11. Click **Add**  .
12. Click **Choose** for “All Criteria”, and then click **Choose** for “Operating System”.
13. Choose “like” from the **Operator** pop-up menu.
14. Type “10.8” in the **Value** field.



15. Choose “and” from the **And/Or** pop-up menu to specify the relationship between the criteria.
16. Click **Save**.

The results of the search are updated each time computers check in with the JSS and meet or fail to meet the specified search criteria.

To view the search results, click **View**.

Viewing Disk Encryption Progress

You can use the advanced computer search you created in “Reporting on FileVault 2-Encrypted Drives” to view disk encryption progress for a FileVault 2-enabled computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
On a smartphone, this option is in the pop-up menu.

4. Click the advanced computer search you created in the “Reporting on File Vault 2-Encrypted Drives” section, and then click **View**.
5. Click the computer you want to view disk encryption progress for.
6. Select **Storage** in the list of categories.

The disk encryption progress is displayed in the FileVault 2 % column.

Viewing FileVault 2 Recovery Keys

You can use the advanced computer search you created in “Reporting on FileVault 2-Encrypted Drives” to view the recovery key for a FileVault 2-enabled computer.

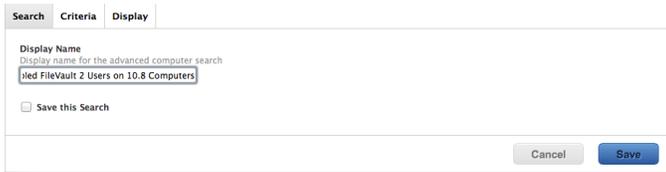
1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
On a smartphone, this option is in the pop-up menu.
4. Click the advanced computer search you created in the “Reporting on File Vault 2-Encrypted Drives” section, and then click **View**.
5. Click the computer you want to view the recovery key for, and then click the **Management** tab.
6. Select **FileVault 2** in the list of categories, and then click **Get Recovery Key**.
 - If the recovery key is an “Individual” recovery key, it is displayed in the JSS.
 - If the recovery key is an “Institutional” recovery key, click **Download** to download it.
 - If the recovery key is an “Individual and Institutional” recovery key, the individual recovery key is displayed in the JSS. To download the institutional recovery key, click **Download**.

Reporting on Enabled FileVault 2 Users

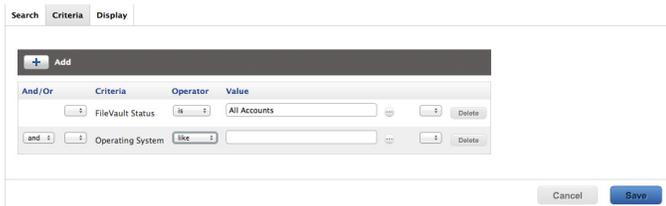
You can create and save an advanced computer search to view the enabled FileVault 2 users on a computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. Use the Search pane to enter a display name for the search.

6. Select the **Save this Search** checkbox.



7. Click the **Criteria** tab.
8. Click **Add** .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault Status".
When the "FileVault Status" criteria is displayed, make sure the operator is set to "Is".
10. Click **Browse** , and then click **Choose** for "All Accounts".
11. Click **Add** .
12. Click **Choose** for "All Criteria", and then click **Choose** for "Operating System".
13. Choose "like" from the **Operator** pop-up menu.
14. Type "10.8" in the **Value** field.



15. Choose "and" from the **And/Or** pop-up menu to specify the relationship between the criteria.
16. Click **Save**.

The results of the search are updated each time computers check in with the JSS and meet or fail to meet the specified search criteria.

To view the search results, click **View**.

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.

1. Restart the target computer.
2. When prompted with the FileVault pre-boot screen, enter credentials for a secondary authorized account.
3. Make sure 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.

1. Restart the target computer 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 convert it to a .keychain file. For instructions, see the following Knowledge Base article:

[Converting a RecoveryKey.p12 File to a FileVaultMaster.keychain File](#)

1. Restart the target computer while pressing Command + R.
This boots the computer to the "Recovery HD" partition.
2. Open Terminal.

3. Unlock the recovery key by executing a command similar to the following:

```
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 a command similar to the following:

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

6. Turn off encryption by executing a command similar to the following:

```
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.

1. Restart the target computer 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.