

Administering FileVault 2 on OS X Mavericks with the Casper Suite v9.2 or Later

Technical Paper
October 2013



 JAMF Software, LLC
© 2013 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.

The Casper Suite, 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 5	Introduction What's in This Guide Important Concepts Additional Resources
Page 6	Overview
Page 7	General Requirements
Page 8	Choosing a Recovery Key
Page 9	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 12	Creating a Disk Encryption Configuration
Page 14	Deploying the Disk Encryption Configuration
Page 16	Creating Smart Computer Groups for FileVault 2 Creating a Smart Group of Computers that are FileVault 2 Encrypted Creating a Smart Group of Computers with a Partition in a Specific Encryption State Creating a Smart Group of Computers that are Not Eligible for FileVault 2 Encryption Creating a Smart Group of Computers with an Invalid Individual Recovery Key Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault 2
Page 22	Viewing FileVault 2 Information for a Computer Viewing FileVault 2 Disk Encryption Information for a Computer Viewing the FileVault 2 Recovery Key for a Computer
Page 24	Issuing a New FileVault 2 Recovery Key Requirements Issuing a New FileVault 2 Recovery Key to Computers

Page 27	Enabling or Disabling a Local Account for FileVault 2 Requirements Enabling a New Local Account for FileVault 2 Disabling an Existing Local Account for FileVault 2
Page 31	Enabling or Disabling the Management Account for FileVault 2 Requirements Enabling or Disabling the Management Account for FileVault 2
Page 33	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 v10.9 with the Casper Suite.

Important Concepts

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

- Deployment
- Smart computer groups

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

This paper provides a complete workflow for administering FileVault 2 on computers with OS X v10.9.

Activating FileVault 2 disk encryption 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.

After activating FileVault 2 disk encryption on computers, you can create smart computer groups to use as the basis for performing the following additional tasks:

- View FileVault 2 information for a computer.
- Issue a new FileVault 2 recovery key to computers.
- Enable or disable a local account for FileVault 2.
- Enable or disable the management account for FileVault 2.
- Access encrypted data.

General Requirements

Administering FileVault 2 on computers requires:

- The JAMF Software Server (JSS) v9.2 or later
- An administrator's computer with OS X v10.8 or later
- Target computers with OS X v10.9 and a "Recovery HD" partition

Note: There are additional requirements for specific procedures covered in this guide.

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 alphanumeric recovery key for each computer. The individual recovery key is generated on the computer and sent back to the JSS for storage 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
```

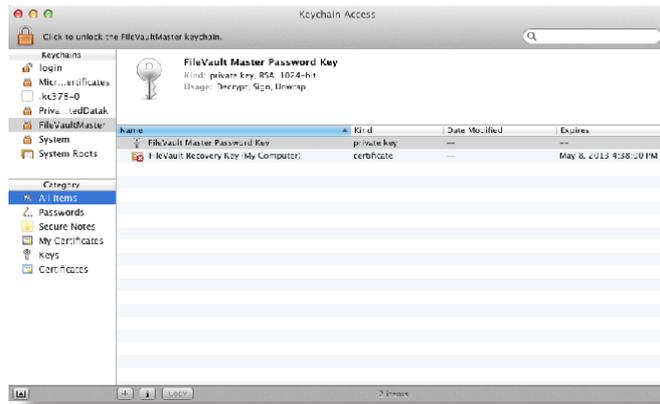
2. Enter a password for the new keychain when prompted.
A keychain (`FileVaultMaster.keychain`) is created in the following location:
`/Library/Keychains/`

3. Unlock the keychain by opening Terminal and executing:

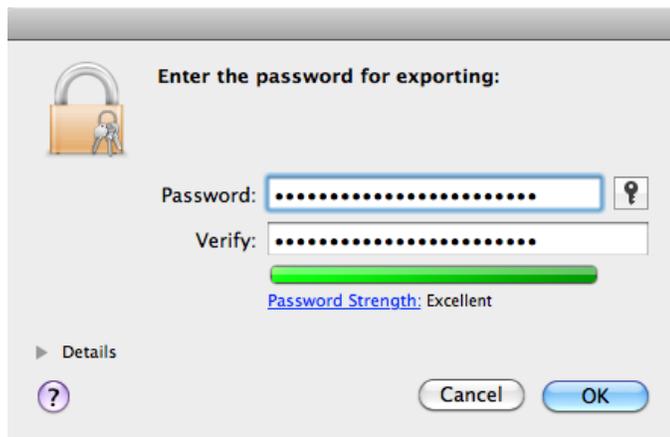
```
security unlock-keychain /Library/Keychains/FileVaultMaster.keychain
```

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
```

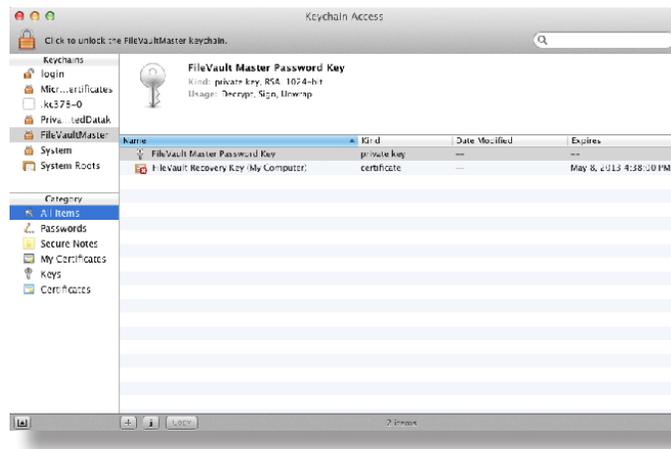
2. Enter a password for the new keychain when prompted.
A keychain (FileVaultMaster.keychain) is created in the following location:
/Library/Keychains/

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.

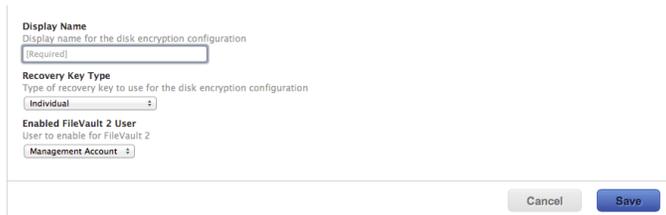
Creating a Disk Encryption Configuration

Creating a disk encryption configuration in the JSS is the first step to activating FileVault 2 on 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

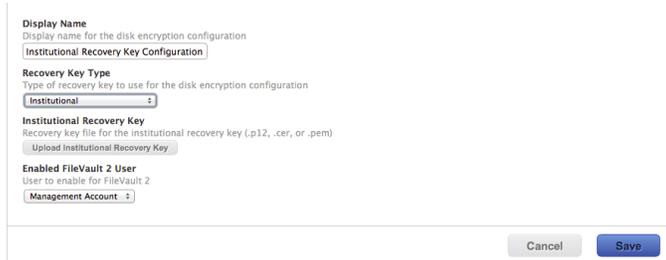
Cancel Save

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

At the bottom right, there 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.

Note: If you make the management account the enabled FileVault 2 user on computers with OS X v10.9, you will be able to issue a new recovery key to those computers later if necessary. (For more information, see [Issuing a New FileVault 2 Recovery Key](#)).

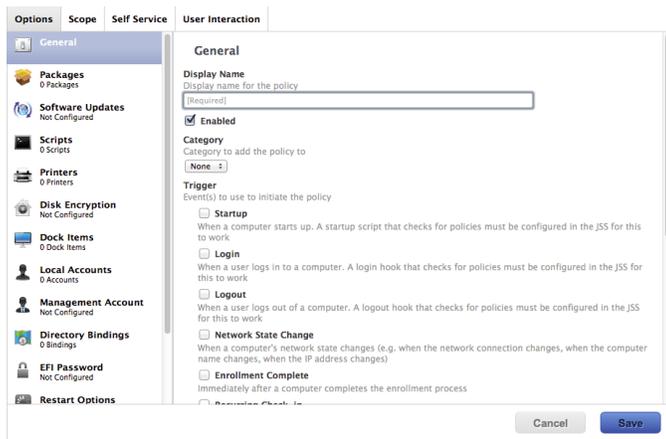
10. Click **Save**.

Deploying the Disk Encryption Configuration

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

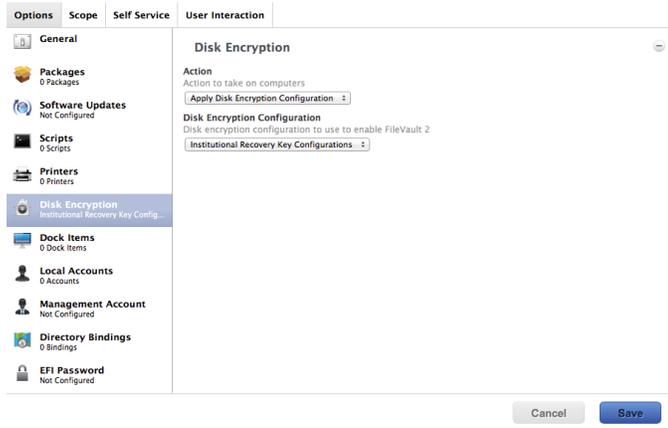
The event that activates FileVault 2 depends on the enabled FileVault 2 user specified in the disk encryption configuration. If the enabled user is “Management Account,” FileVault 2 is activated on a computer the next time the computer restarts. If the enabled user is “Current or Next User,” FileVault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

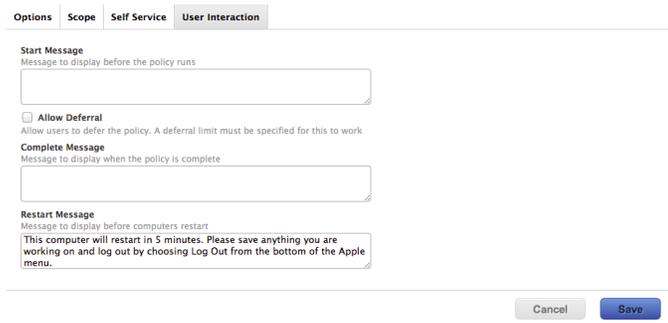


6. Select a trigger.
7. Choose “Once per computer” from the **Execution Frequency** pop-up menu.
8. Select the Disk Encryption payload and click **Configure**.

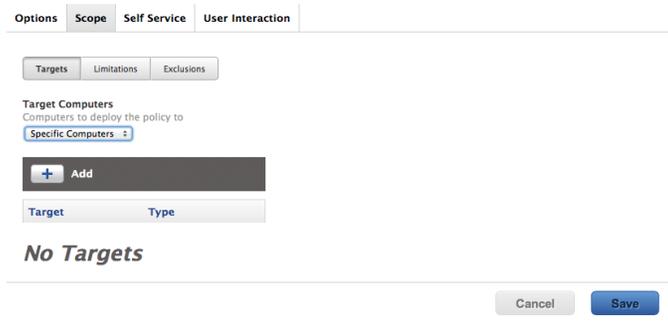
9. Choose “Apply Disk Encryption Configuration” from the **Action** pop-up menu.
10. Choose the disk encryption configuration from the **Disk Encryption Configuration** pop-up menu.



11. If “Management Account” is selected as the enabled FileVault 2 user in the disk encryption configuration, do the following:
 - a. Select the Restart Options payload and configure restart settings for the computer.
 - b. (Optional) Click the **User Interaction** tab and customize the restart message displayed to users.



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



13. 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.

Creating Smart Computer Groups for FileVault 2

You can use the JSS to create smart computer groups that can be used as the scope of FileVault 2 tasks. FileVault 2 smart computer groups can be based on the following criteria:

- Computers that are FileVault 2 encrypted
- Computers that are in a specific FileVault 2 partition encryption state
- Computers that are not eligible to be FileVault 2 encrypted
- Computers with an invalid individual recovery key
- Computers on which a specified user is enabled for FileVault 2

After creating a smart computer group, you can view its memberships.

Note: You can create smart computer groups based on additional FileVault 2 criteria that are not covered in this guide. For information on all FileVault 2 smart group criteria, see the following Knowledge Base article:

[Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault](#)

Creating a Smart Group of Computers that are FileVault 2 Encrypted

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault 2 Status".
When the criteria is displayed, make sure the operator is set to "is".

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



11. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating Smart Groups of Computers with a Partition in a Specific Encryption State

You can create a smart group of computers with a partition that is in any of the following encryption states:

- Decrypted
- Decrypting
- Encrypted
- Encrypting
- Ineligible
- Not Encrypted
- Unknown

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** .

9. Click **Choose** for “All Criteria”, and then click **Choose** for “Partition Name”.
10. Choose “has” from the **Operator** pop-up menu.
11. Type a partition name in the **Value** field, or click **Browse**  and then click **Choose** for “Boot Partition”.



12. Click **Add**  .
13. Click **Choose** for “All Criteria”, and then click **Choose** for “FileVault 2 Partition Encryption State”. When the criteria is displayed, make sure the operator is set to “is”.
14. Click **Browse** , and then click **Choose** for the encryption state you want to base the group on.



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

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Creating a Smart Group of Computers that are Not Eligible for FileVault 2 Encryption

You can create a smart group of computers that do not have an institutional recovery key.

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

4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault 2 Eligibility".
10. Choose "is not" from the **Operator** pop-up menu.
11. Click **Browse** , and then click **Choose** for "Eligible".



12. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group's membership, click **View**.

Creating a Smart Group of Computers with an Invalid Individual Recovery Key

You can create a smart computer group to validate that the individual recovery key on computers matches the key stored in the JSS.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.

7. Click the **Criteria** tab.
8. Click **Add** .
9. Click **Choose** for "All Criteria", and then click **Choose** for "FileVault 2 Individual Key Validation". When the criteria is displayed, make sure the operator is set to "is".
10. Click **Browse** , and then click **Choose** for "Invalid".



11. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group's membership, click **View**.

Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault 2

You can create a smart computer group to identify the computers for which a specified user is enabled for FileVault 2.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the group.
6. To enable email notifications, select the **Send email notification on membership change** checkbox.
7. Click the **Criteria** tab.
8. Click **Add** .

9. Click **Choose** for “All Criteria”, and then click **Choose** for “FileVault 2 User”.
When the criteria is displayed, make sure the operator is set to “has”.
10. Enter a username, or click **Browse**  and then click **Choose** for a FileVault 2-enabled user.



11. Click **Save**.

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group’s membership, click **View**.

Viewing FileVault 2 Information for a Computer

You can view the FileVault 2 disk encryption information for a computer. You can also view its FileVault 2 recovery key.

Viewing FileVault 2 Disk Encryption Information for a Computer

You can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 2 Encrypted” to view the following information for the boot partition on a FileVault 2-encrypted computer:

- Last inventory update
- FileVault 2 partition encryption state
- Individual recovery key validation
- Institutional recovery key
- Disk encryption configuration
- FileVault 2-enabled users

You can also view the last inventory update date and partition encryption state for any non-boot partitions on the computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 2 Encrypted”, and then click **View**.
5. Click the computer you want to view disk encryption information for.
6. Select **Disk Encryption** in the list of categories.

The computer’s FileVault 2 disk encryption information is displayed for the boot partition. For any additional partitions, the last inventory update date and partition encryption state is displayed.

Viewing the FileVault 2 Recovery Key for a Computer

You can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 2 Encrypted” to view the recovery key for a FileVault 2-encrypted computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click the smart computer group you created in the “Creating a Smart Group of Computers that are FileVault 2 Encrypted” 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**.

Issuing a New FileVault 2 Recovery Key

You can use a policy to issue a new FileVault 2 recovery key to computers with OS X v10.9 that have FileVault 2 activated. This allows you to do the following:

- Replace an individual recovery key that has been reported as invalid and does not match the recovery key stored in the JSS.
- Update the recovery key on computers on a regular schedule, without needing to decrypt and then re-encrypt the computers.

Requirements

To issue a new individual recovery key to a computer, the computer must have:

- OS X v10.9
- A “Recovery HD” partition
- FileVault 2 activated
- One of the following conditions met:
 - The management account configured as the FileVault 2-enabled user
 - An existing, valid individual recovery key that matches the key stored in the JSS

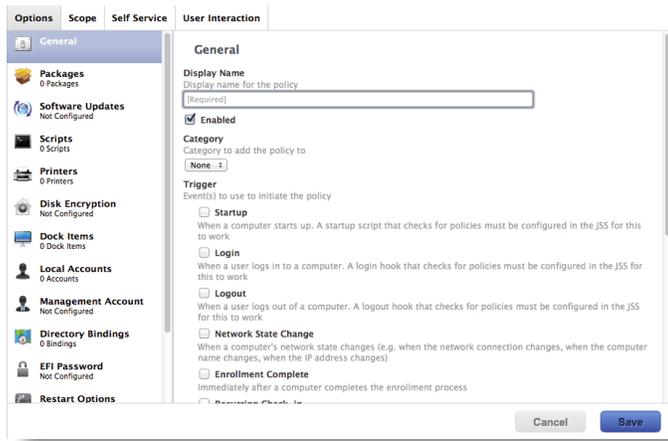
To issue a new institutional recovery key to a computer, the computer must have:

- OS X v10.9
- A “Recovery HD” partition
- FileVault 2 activated
- The management account configured as the FileVault 2-enabled user

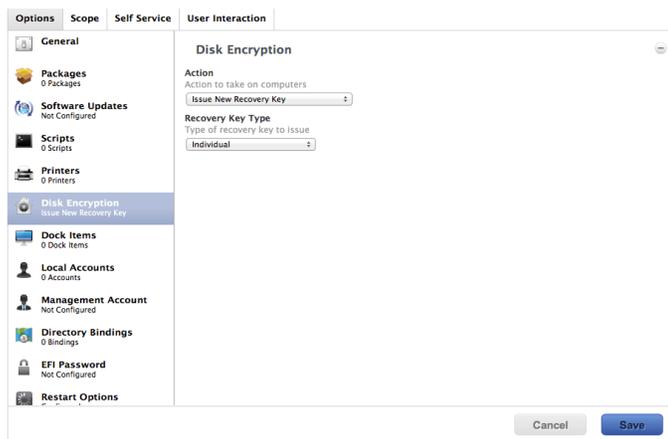
Issuing a New FileVault 2 Recovery Key to Computers

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**  .

- In the General payload, enter a display name for the policy. For example, "FileVault 2 New Individual Recovery Key".

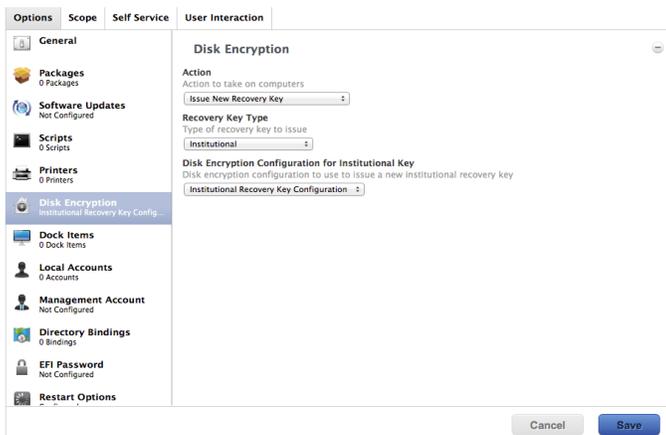


- Select a trigger and execution frequency.
- Select the Disk Encryption payload and click **Configure**.
- Choose "Issue New Recovery Key" from the **Action** pop-up menu.



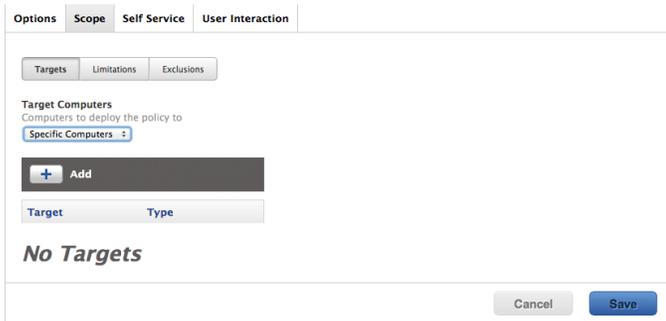
- Choose the type of recovery key you want to issue from the **Recovery Key Type** pop-up menu:
 - Individual**—A new individual recovery key is generated on each computer and then submitted to the JSS for storage.
 - Institutional**—A new institutional recovery key is deployed to computers and stored in the JSS.
 - Individual and Institutional**—Issues both types of recovery keys to computers.

If you chose “Institutional” or “Individual and Institutional”, choose the disk encryption configuration to use to issue the new recovery key from the **Disk Encryption Configuration for Institutional Key** pop-up menu.



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

Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers with an Invalid Individual Recovery Key” as the scope for the policy.



11. 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.

Enabling or Disabling a Local Account for FileVault 2

When you create a new account, you can enable the account for FileVault 2. You can also disable an existing account for FileVault 2.

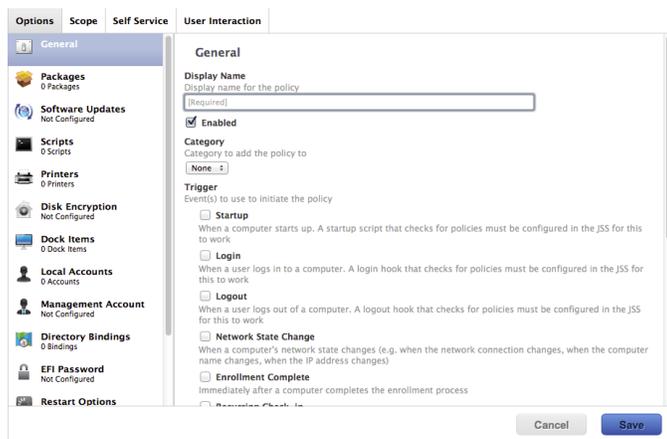
Requirements

To enable a new account for FileVault 2, the computer must have OS X v10.9 and have an existing, valid individual recovery key that matches the key stored in the JSS.

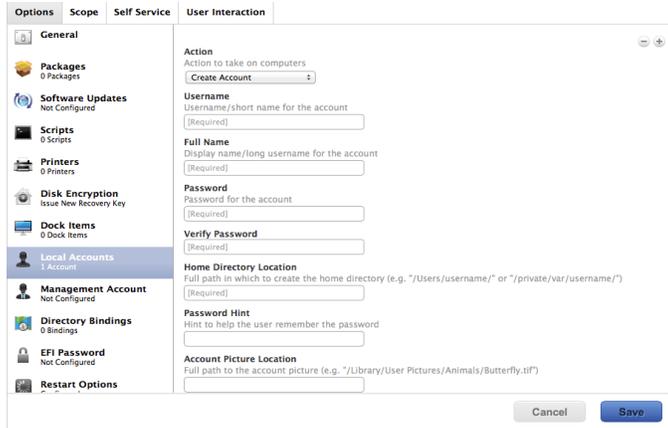
To disable an existing account for FileVault 2, the computer must have OS X v10.9.

Enabling a New Local Account for FileVault 2

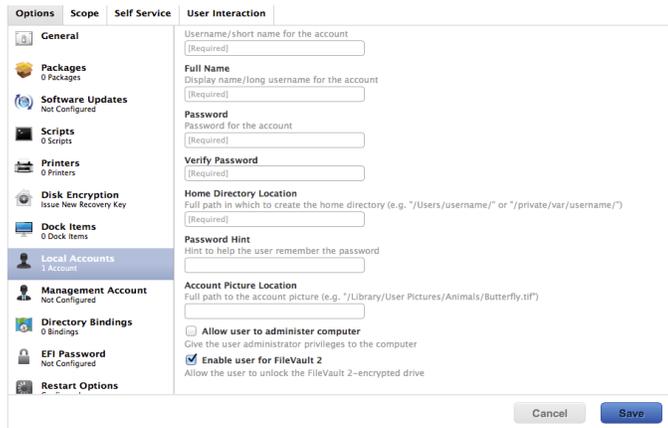
1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
On a smartphone, this option is in the pop-up menu.
4. Click **New**  .
5. In the General payload, enter a display name for the policy. For example, "Add Local Account for FileVault 2".



6. Select a trigger and execution frequency.
7. Select the Local Accounts payload and click **Configure**.
8. Choose "Create Account" from the **Action** pop-up menu.



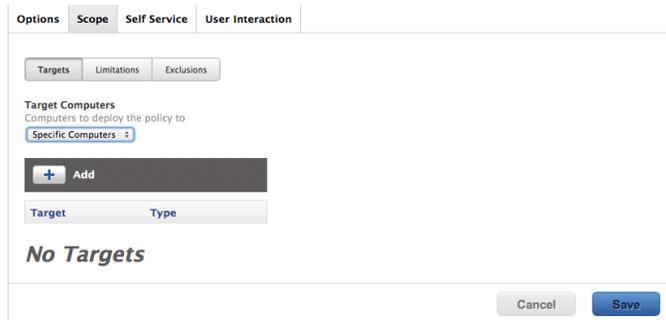
9. Specify the required information for the local account, including the username, full name, password, and home directory location.
10. Select the **Enable user for FileVault 2** checkbox.



11. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault 2-enabled status for the user is updated in inventory immediately when the policy runs.

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

Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 2 Encrypted” as the scope for the policy.

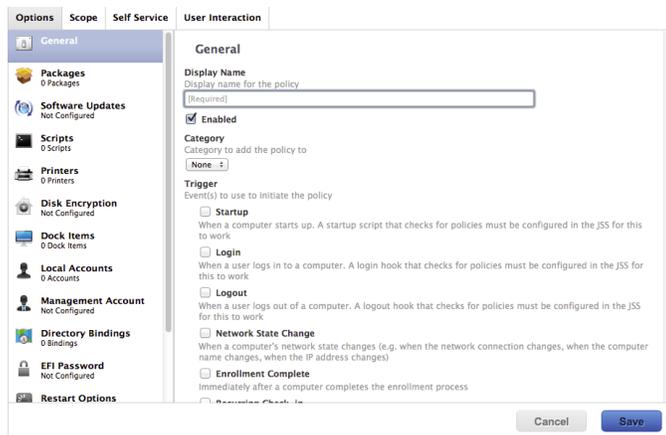


13. Click **Save**.

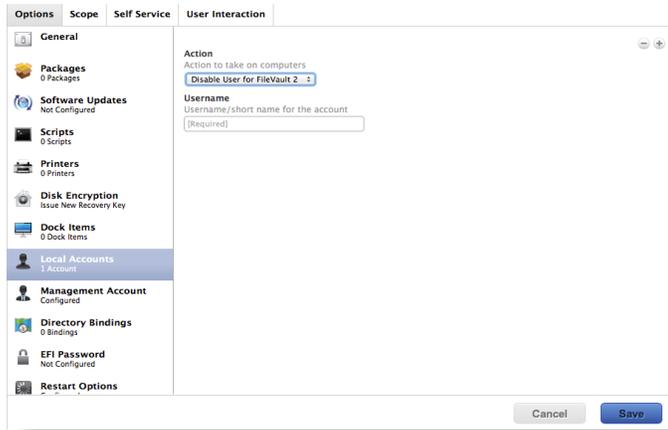
The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Disabling an Existing Local Account for FileVault 2

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, “Disable Local Account for FileVault 2”.

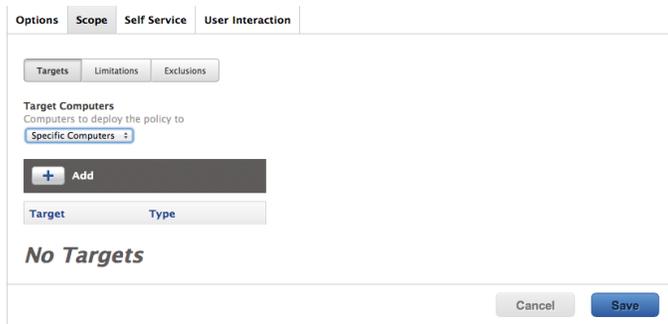


6. Select a trigger and execution frequency.
7. Select the Local Accounts payload and click **Configure**.
8. Choose “Disable User for FileVault 2” from the **Action** pop-up menu.



9. Enter the username of the user you want to disable for FileVault 2.
10. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault 2 Enabled status for the local account is updated in inventory immediately when the policy runs.
11. Click the **Scope** tab and configure the scope of the policy.

Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault 2” as the scope for 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.

Enabling or Disabling the Management Account for FileVault 2

You can enable or disable the management account for FileVault 2.

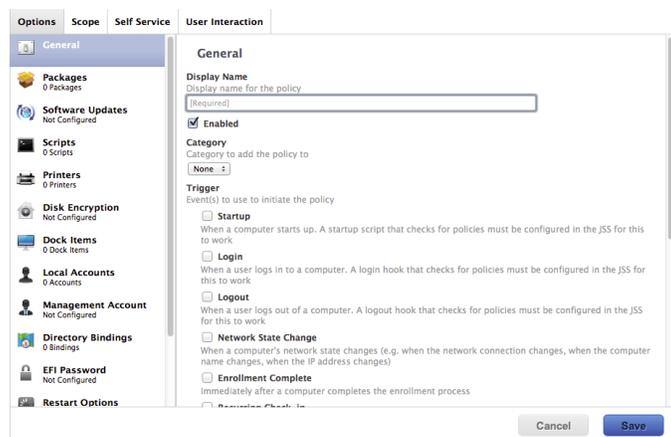
Requirements

To enable the management account for FileVault 2, the computer must have OS X v10.9 and have an existing, valid individual recovery key that matches the key stored in the JSS.

To disable the management account for FileVault 2, the computer must have OS X v10.9.

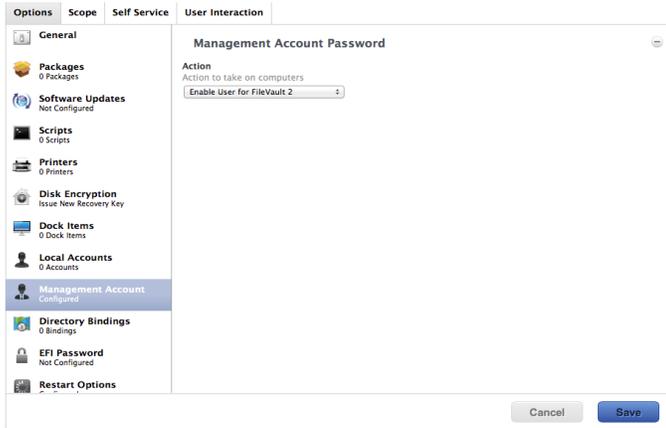
Enabling or Disabling the Management Account for FileVault 2

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, "Enable Management Account for FileVault 2".



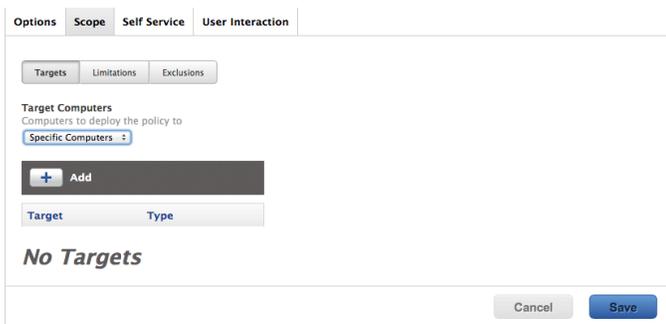
6. Select a trigger and execution frequency.

7. Select the Management Account payload and click **Configure**.
8. Choose “Enable User for FileVault 2” or “Disable User for FileVault 2” from the **Action** pop-up menu.



9. (Optional) Select the Maintenance payload and then select the **Update Inventory** checkbox so that the FileVault 2 Enabled status for the management account is updated in inventory immediately when the policy runs.
10. Click the **Scope** tab and configure the scope of the policy.

Note: If applicable, you can use the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 2 Encrypted” as the scope for the policy.



11. 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.

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.