

# Administering FileVault on macOS 10.14 or Later with Jamf Pro

Technical Paper  
Jamf Pro 9.81 or Later  
15 October 2018



© copyright 2002-2018 Jamf. All rights reserved.

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

Jamf  
100 Washington Ave S Suite 1100  
Minneapolis, MN 55401-2155  
(612) 605-6625

Jamf, the Jamf Logo, JAMF SOFTWARE®, and the JAMF SOFTWARE Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

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

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

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

# Contents

## **4 Introduction**

- 4 What's in This Guide
- 4 Important Concepts
- 4 Additional Resources

## **5 Overview**

## **6 General Requirements**

## **7 Activating FileVault Disk Encryption Using a Configuration Profile**

## **8 Choosing a Recovery Key**

## **9 Creating and Exporting an Institutional Recovery Key**

- 9 Creating and Exporting an Institutional Recovery Key with the Private Key
- 10 Creating and Exporting an Institutional Recovery Key without the Private Key

## **12 Creating a Disk Encryption Configuration**

## **14 Deploying the Disk Encryption Configuration**

## **19 Creating Smart Computer Groups for FileVault**

- 19 Creating a Smart Group for FileVault Eligible Computers that are Not Yet Encrypted
- 21 Creating Smart Groups of Computers with a Partition in a Specific Encryption State
- 23 Creating a Smart Group of Computers that are Not Eligible for FileVault Encryption
- 24 Creating a Smart Group of Computers with an Invalid Individual Recovery Key
- 25 Creating a Smart Group of Computers for Which a Specified User is Enabled for FileVault

## **26 Viewing FileVault Information for a Computer**

- 26 Viewing FileVault Disk Encryption Information for a Computer
- 27 Viewing the FileVault Recovery Key for a Computer

## **28 Issuing a New FileVault Recovery Key**

- 28 Requirements
- 28 Issuing a New FileVault Recovery Key to Computers

# Introduction

## What's in This Guide

This guide provides step-by-step instructions for administering FileVault on macOS 10.14 or later with Jamf Pro.

## Important Concepts

Administrators using this guide should be familiar with the following Jamf Pro-related concepts:

- Deployment
- Smart computer groups

## Additional Resources

For more information on related topics, see the [Jamf Pro Administrator's Guide](#).

# Overview

This paper provides a complete workflow for administering FileVault on computers with macOS 10.14 or later.

FileVault disk encryption can be activated using a configuration profile or by performing 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 disk encryption on computers, you can create smart computer groups to use as the basis for performing the following tasks:

- View FileVault information for a computer.
- Issue a new FileVault recovery key to computers.

# General Requirements


Performing the administrative tasks in this paper requires the following::

- Jamf Pro 9.81 or later
- An administrator computer with macOS 10.11 or later
- Target computers with macOS 10.14 or later and a “Recovery HD” partition

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

# Activating FileVault Disk Encryption Using a Configuration Profile

You can activate FileVault disk encryption using a configuration profile. Disk encryption configuration will deploy at next user logout.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
4. Click **New**  .
5. Use the General payload to configure basic settings, which includes the distribution method. This configuration profile payload can only be applied at the Computer Level. Only payloads and settings that apply to the selected level are displayed for the profile.
6. Use the Security & Privacy payload to configure FileVault settings.
  - a. Click the **FileVault** tab.
  - b. Select the **Require FileVault 2** checkbox.
  - c. Select **Use institutional recovery key**, **Create individual recovery key**, or both.
  - d. (Optional) If you are using an institutional key, select the certificate that contains the public key from institutional recovery keychain. You can use the Certificate payload to upload an institutional recovery key to Jamf Pro.
  - e. (Optional) If you are using an individual recovery key on macOS 10.14 or later, select **Enable Escrow Personal Recovery Key** to enable the device to encrypt the personal recovery key with the provided certificate and report it to Jamf Pro.
7. (Optional) Use the rest of the payloads to configure the settings you want to apply.
8. Click the **Scope** tab and configure the scope of the profile.
9. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
10. Click **Save**.

# Choosing a Recovery Key

The first step to administering FileVault 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 Jamf Pro for storage when the encryption takes place. This type of recovery key can function as a password and can be used to unlock the computer.
- **Institutional**—Uses a shared recovery key. This requires you to create the recovery key with Keychain Access and upload to Jamf Pro for storage. This type of recovery key cannot be used to unlock a user's startup disk.

You can choose to use both recovery keys (individual and institutional) together in Jamf Pro.

If you plan to use an institutional recovery key, you must first create an 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 Jamf Pro. 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:

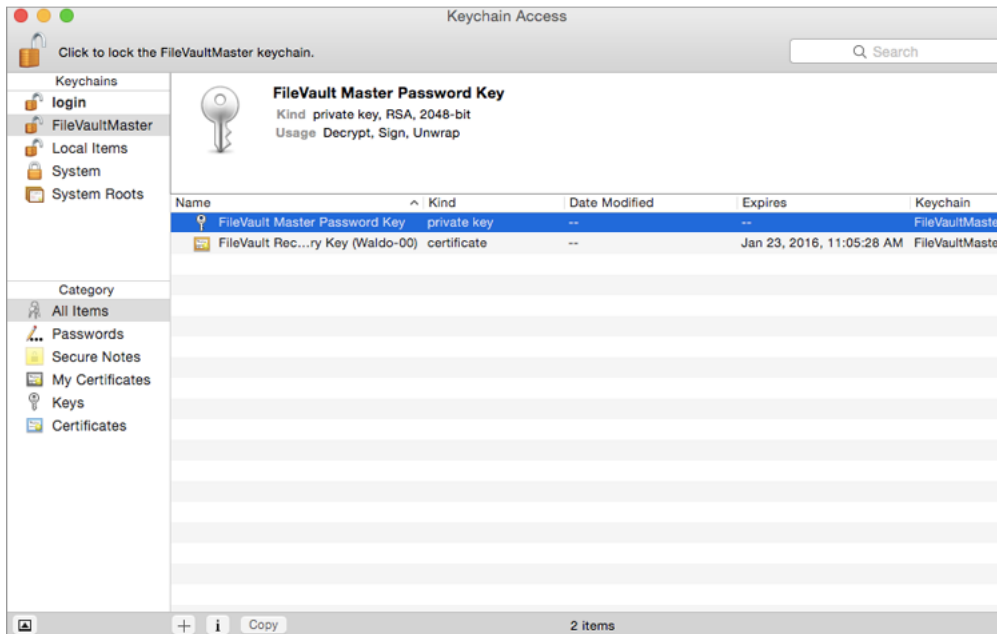
```
sudo security create-filevaultmaster-keychain /Library/Keychains/  
FileVaultMaster.keychain
```

2. When prompted, enter a password for the new keychain when prompted.
3. To unlock the keychain, open Terminal and execute the following command:

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

4. Perform a backup of the keychain and save it in a secure location.
5. Open Keychain Access.
6. From the menu bar, choose "Add Keychain" from the **File** pop-up menu. Then, add the `FileVaultMaster.keychain` file located in `/Library/Keychains/`.
7. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading.

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



9. Select the certificate and the private key.
10. From the menu bar, choose "Export Items" from the **File** pop-up menu. Then, save the items as a .p12 file.  
The .p12 file is a bundle that contains both the FileVault Recovery Key and the private key.
11. Create and verify a password to secure the file, and then click **OK**.  
You will be prompted to enter this password when uploading the recovery key to Jamf Pro.
12. Quit Keychain Access.
13. Store the keychain (FileVaultMaster.keychain) in a secure location so you can use it to access encrypted data at a later time. Without the keychain, you will not be able to decrypt the computer.

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:

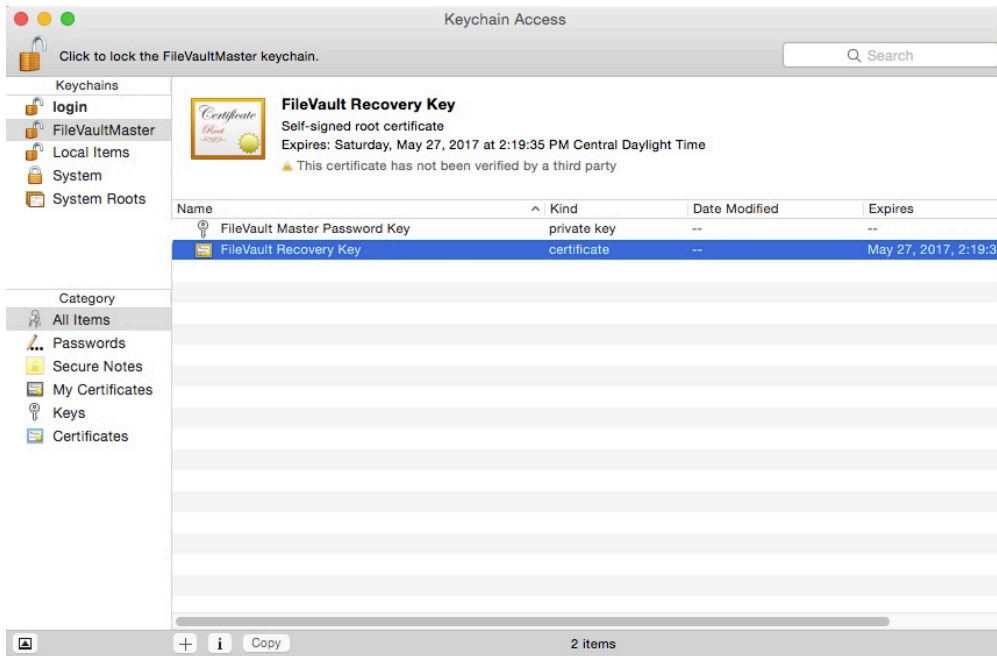
```
sudo security create-filevaultmaster-keychain /Library/Keychains/  
FileVaultMaster.keychain
```

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. From the menu bar, choose "Add Keychain" from the **File** pop-up menu. Then, add the FileVaultMaster.keychain file located in /Library/Keychains/.
6. Select **FileVaultMaster** under the Keychains heading in the sidebar, and then select **All Items** under the Category heading.
7. Select the certificate. Do not select the private key associated with the certificate.



8. From the menu bar, choose "Export Items" from the **File** pop-up menu. Then, save the recovery key as a .pem file or .cer file.  
You will need to upload this file to Jamf Pro when creating the disk encryption configuration.
9. Quit Keychain Access.
10. 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.

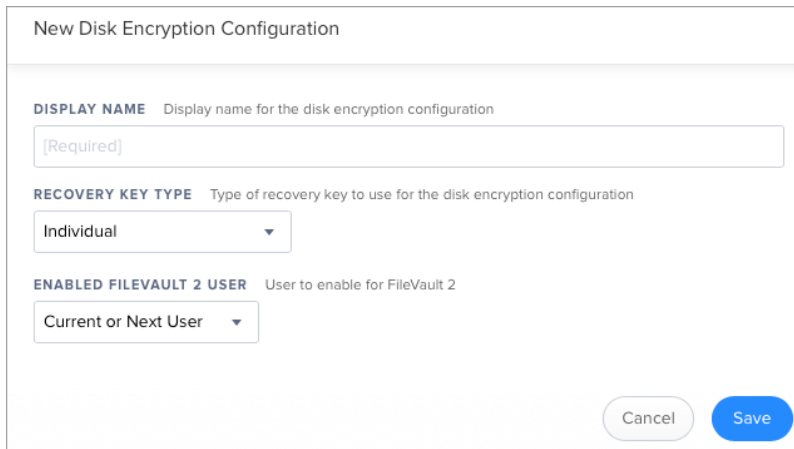
# Creating a Disk Encryption Configuration

Creating a disk encryption configuration in Jamf Pro is the first step to activating FileVault 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

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
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.



New Disk Encryption Configuration

**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  
Current or Next User

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 Jamf Pro. 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.

New Disk Encryption Configuration

**DISPLAY NAME** Display name for the disk encryption configuration

Institutional Recovery Key Configuration

**RECOVERY KEY TYPE** Type of recovery key to use for the disk encryption configuration

Institutional

**INSTITUTIONAL RECOVERY KEY**  
Recovery key file for the institutional recovery key (.p12, .cer, or .pem)

Upload Institutional Recovery Key

**ENABLED FILEVAULT 2 USER** User to enable for FileVault 2

Current or Next User

Cancel Save

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


# Deploying the Disk Encryption Configuration

The event that activates FileVault depends on the enabled FileVault user specified in the disk encryption configuration and whether the computer is APFS enabled. If the enabled user is "Management Account", and the computer is APFS enabled, FileVault is activated on a computer at the next login without needing to reboot. If the computer is HFS+ formatted, with the "Management Account" enabled user, FileVault is activated on a computer the next time the computer restarts. If the enabled user is "Current or Next User", you can modify when FileVault is activated on a computer. Options include the following:

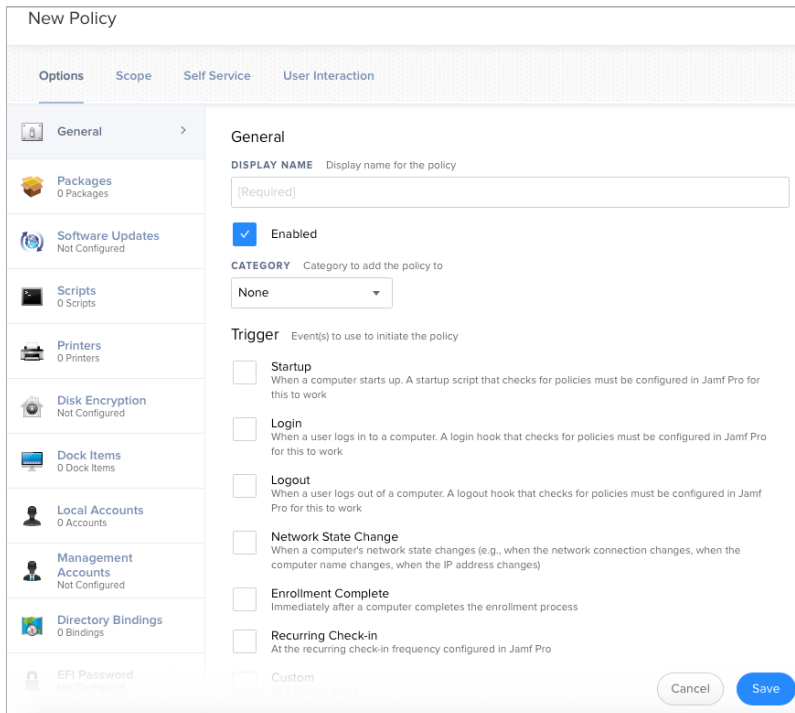
- The next time the computer restarts.
- The next time the current user logs out.
- The next login or after multiple user logins, ranging from two to six logins.

**Note:** If the restart is done via a built-in policy, FileVault will not be activated.

Deploying the disk encryption configuration involves the following steps:

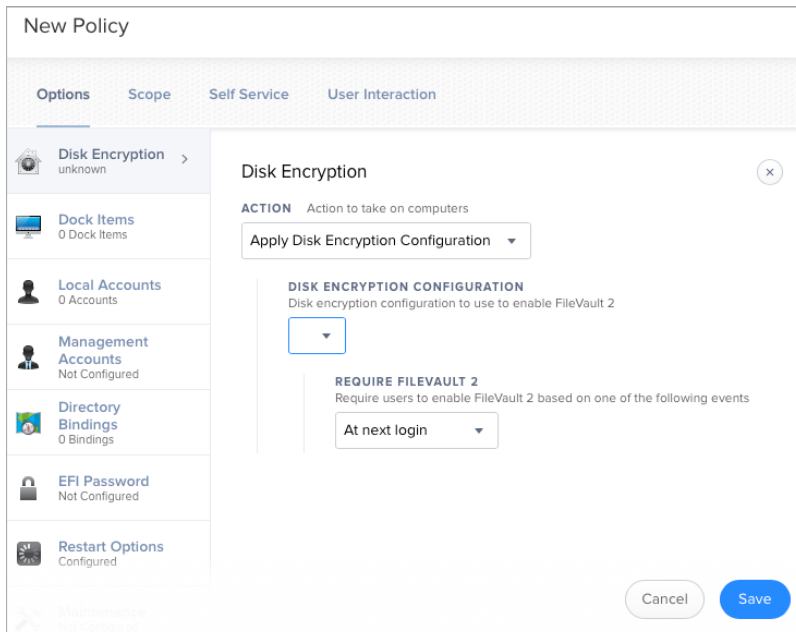
1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New**  .

5. In the General payload, enter a display name for the policy. For example, “FileVault Disk Encryption”.



6. Select a trigger.
7. Choose “Ongoing” 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. Choose an event from the **Require FileVault 2** pop-up menu to specify when users must enable disk encryption.





12. If "Management Account" is selected as the enabled FileVault user in the disk encryption configuration, do the following:
  - a. Select the Restart Options payload and configure restart settings for the computer.  
**Note:** Select "Restart" from the appropriate pop-up menu to include a restart prompt. Select "Restart immediately" to restart without prompting. "Restart" option does not work if set to encrypt at logout.
  - b. (Optional) Click the **User Interaction** tab and customize the restart message displayed to users.

The screenshot shows a 'New Policy' configuration window with four tabs: 'Options', 'Scope', 'Self Service', and 'User Interaction'. The 'User Interaction' tab is selected. It contains three message fields: 'START MESSAGE' (empty), 'COMPLETE MESSAGE' (empty), and 'RESTART MESSAGE' (pre-filled with the text: 'This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple menu.'). There is also an 'Allow Deferral' checkbox which is unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons.

In an upcoming release of Jamf Pro, you can select **Perform authenticated restart on computers with FileVault 2 enabled** to allow computers with macOS 10.8.2 or later that are FileVault enabled to be restarted without requiring an unlock the next time the computer starts. This affects future reboots, but does not apply to the setup of the original encryption policy.

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

New Policy

Options **Scope** Self Service User Interaction

Targets Limitations Exclusions

**TARGET COMPUTERS**  
Computers to deploy the policy to  
Specific Computers

**TARGET USERS**  
Users to deploy the policy to  
Specific Users

Selected Deployment Targets + Add

TARGET	TYPE
No Targets	

Cancel Save

**Note:** It is recommended that the scope of this policy includes a smart group with computers that are FileVault eligible, but are not yet encrypted. For information on how to create this smart group, see [Creating Smart Computer Groups for FileVault](#).

14. Click **Save**.

The policy runs on computers in the scope the next time they check in with Jamf Pro and match the selected trigger in the General payload.

# Creating Smart Computer Groups for FileVault



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


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

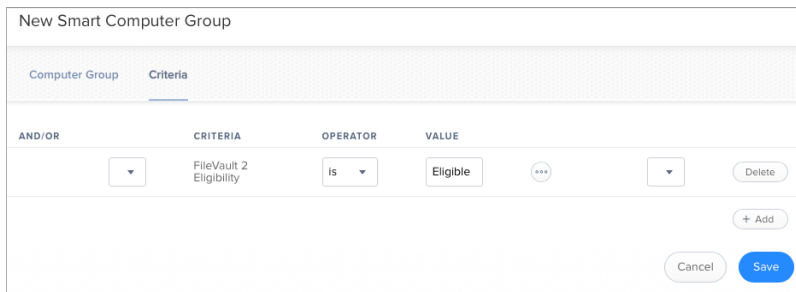
After creating a smart computer group, you can view its memberships.

**Note:** You can create smart computer groups based on additional FileVault criteria that are not covered in this guide. For information on all FileVault smart group criteria, see the [Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault](#) Knowledge Base article.

## Creating a Smart Group for FileVault Eligible Computers that are Not Yet Encrypted

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Show Advanced Criteria**, and then click **Choose** for “FileVault 2 Eligibility”. When the criteria is displayed, make sure the operator is set to “is”.



10. Click **Browse** , and then click **Choose** for “Eligible”.

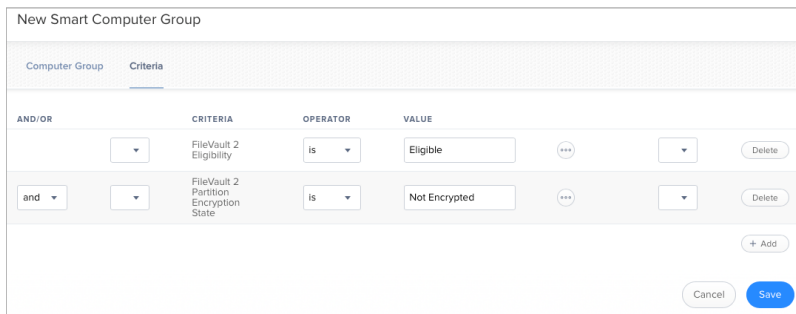


AND/OR	CRITERIA	OPERATOR	VALUE		
	FileVault 2 Eligibility	is	Eligible	⋮	Delete

+ Add

Cancel Save

11. Click **Add**  .
12. Click **Show Advanced Criteria**, and then click **Choose** for “FileVault 2 Partition Encryption State”. When the criteria is displayed, make sure the operator is set to “is”.
13. Click **Browse** , and then click **Choose** for “Not Encrypted”.



AND/OR	CRITERIA	OPERATOR	VALUE		
	FileVault 2 Eligibility	is	Eligible	⋮	Delete
and	FileVault 2 Partition Encryption State	is	Not Encrypted	⋮	Delete

+ Add

Cancel Save

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



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


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

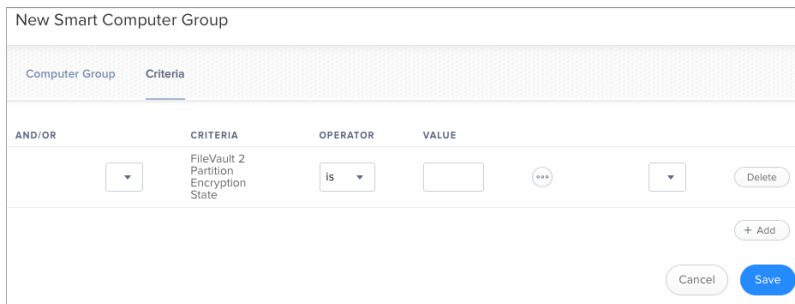
# Creating Smart Groups of Computers with a Partition in a Specific Encryption State

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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Show Advanced Criteria**, and then click **Choose** for “FileVault 2 Partition Encryption State”. When the criteria is displayed, make sure the operator is set to “is”.

10. Click **Browse** , and then click **Choose** for the encryption state you want to base the group on.



AND/OR	CRITERIA	OPERATOR	VALUE
<input type="checkbox"/>	FileVault 2 Partition Encryption State	is <input type="checkbox"/>	<input type="text"/>




11. Click **Save**.

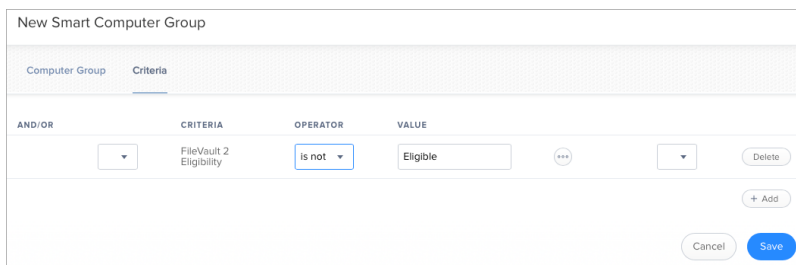
Group memberships are updated each time computers check in with Jamf Pro and meet or fail to meet the specified criteria.


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

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

You can create a smart group of computers that are not eligible for FileVault Encryption.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Show Advanced 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”.



AND/OR	CRITERIA	OPERATOR	VALUE		
<input type="checkbox"/>	FileVault 2 Eligibility	is not	Eligible		<input type="checkbox"/> Delete




12. Click **Save**.

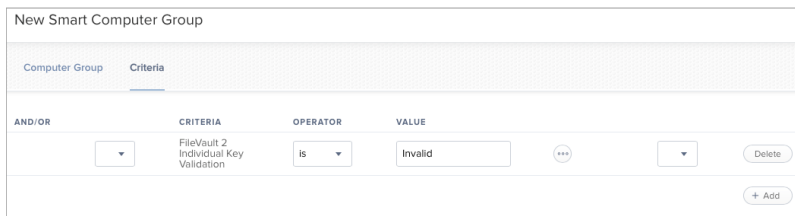
Group memberships are updated each time computers check in with Jamf Pro and meet or fail to meet the specified criteria.

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 Jamf Pro.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Show Advanced 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”.



AND/OR	CRITERIA	OPERATOR	VALUE	
<input type="button" value="v"/>	FileVault 2 Individual Key Validation	is <input type="button" value="v"/>	Invalid <input type="text"/>	<input type="button" value="..."/> <input type="button" value="Delete"/>
<input type="button" value="+ Add"/>				

11. Click **Save**.




Group memberships are updated each time computers submit inventory with Jamf Pro and meet or fail to meet the specified criteria.

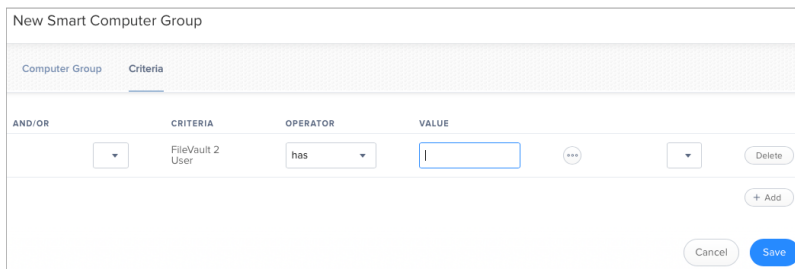
To view the group’s membership, click **View**.



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

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

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
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 **Show Advanced 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.



AND/OR	CRITERIA	OPERATOR	VALUE
<input type="checkbox"/>	FileVault 2 User	has	

Buttons: Delete, + Add, Cancel, Save

11. Click **Save**.

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

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

# Viewing FileVault Information for a Computer

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

## Viewing FileVault 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 Encrypted” to view the following information for the boot partition on a FileVault-encrypted computer:

- Last inventory update
- FileVault partition encryption state
- Individual recovery key validation
- Institutional recovery key
- Disk encryption configuration
- FileVault-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 Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click the smart computer group you created in “Creating a Smart Group of Computers that are FileVault 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 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 Recovery Key for a Computer

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

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
4. Click the smart computer group you created in the “Creating a Smart Group of Computers that are FileVault 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 Jamf Pro.
  - 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 Jamf Pro. To download the institutional recovery key, click **Download**.

**Note:** When a user views the FileVault Recovery Key, it logs their the username and the date and time viewed in the “Viewed FileVault Encryption Key”.

# Issuing a New FileVault Recovery Key

You can use a policy to issue a new FileVault recovery key to computers with macOS 10.14 or later that have FileVault 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 Jamf Pro.
- 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:

- macOS 10.14 or later
- A "Recovery HD" partition
- FileVault activated

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

- macOS 10.14 or later
- A "Recovery HD" partition
- FileVault enabled

## Issuing a New FileVault Recovery Key to Computers

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New**  .

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

New Policy

Options Scope Self Service User Interaction

General

DISPLAY NAME Display name for the policy  
[Required]

Enabled

CATEGORY Category to add the policy to  
None

Trigger Event(s) to use to initiate the policy

Startup  
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

Login  
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

Logout  
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

Network State Change  
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

Enrollment Complete  
Immediately after a computer completes the enrollment process

Recurring Check-in  
At the recurring check-in frequency configured in Jamf Pro

Custom  
Custom (not supported)

Cancel Save

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

FileVault New Individual Recovery Key

Options Scope Self Service User Interaction

Disk Encryption

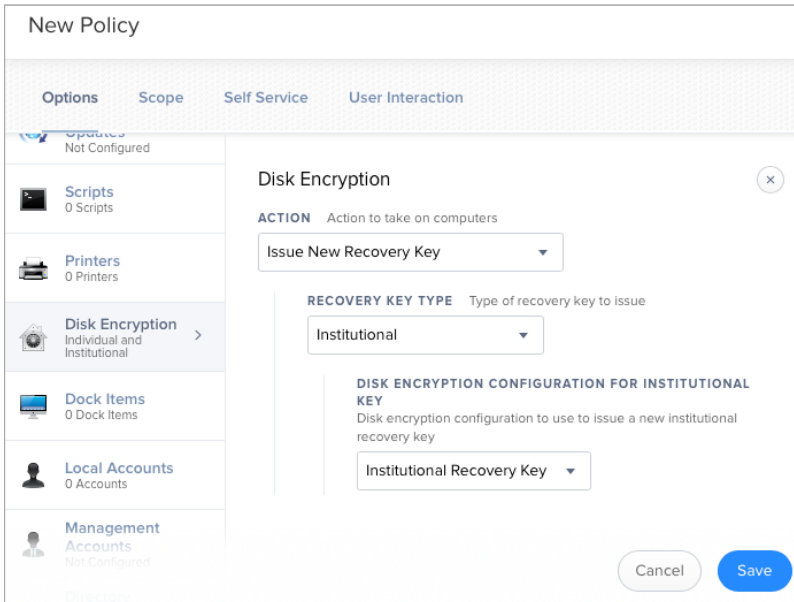
ACTION Action to take on computers  
Issue New Recovery Key

RECOVERY KEY TYPE Type of recovery key to issue  
Individual

Cancel Save

9. 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 Jamf Pro for storage.
  - **Institutional**—A new institutional recovery key is deployed to computers and stored in Jamf Pro.
  - **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.

The screenshot shows the 'FileVault New Individual Recovery Key' configuration page with the 'Scope' tab selected. The page has a navigation bar with 'Options', 'Scope', 'Self Service', and 'User Interaction'. Below the navigation bar are three tabs: 'Targets', 'Limitations', and 'Exclusions'. Under the 'Targets' tab, there are two sections: 'TARGET COMPUTERS' (Computers to deploy the policy to) with a dropdown menu set to 'Specific Computers', and 'TARGET USERS' (Users to deploy the policy to) with a dropdown menu set to 'Specific Users'. Below these is a 'Selected Deployment Targets' section with a '+ Add' button. At the bottom, there is a table with columns 'TARGET' and 'TYPE' containing the text 'No Targets'. At the very bottom are 'Cancel' and 'Save' buttons.

11. Click **Save**.

The policy runs on computers in the scope the next time they check in with Jamf Pro, prompting enabled users.