



How to Reissue a Recovery Key for Filevault

To follow along with this guide, you will need the following items:

- Jamf Pro Server
- Rich Trouton's FileVault status extension attribute: <http://goo.gl/zB04LT>
Download this file: `filevault_2_encryption_check_extension_attribute.sh`
- Elliot Jordan - Homebysix: `jss-filevault-reissue`: <https://goo.gl/liKxav>
Download this file: `reissue_filevault_recovery_key.sh`

Feel free to use the sample files used to create this guide and edit them to meet your needs.

Special thanks to Elliot Jordan and Rich Trouton for all their contributions to the Apple community.

Section 1 Configuring Security Settings

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.
4. In the "Computer Management-Management Framework" section, click Security .
5. Click Edit.
6. Confirm the "Enable push notifications" is checked
7. Click Save.

Security

☒ **Enable certificate-based authentication**
Ensure that the JSS verifies that device certificates on computers are valid

☒ **Enable push notifications**
Allow the JSS to send push notifications to Mac computers. This requires a push certificate and is required for macOS configuration profiles and macOS remote commands to work

SSL Certificate Verification
Ensure that computers verify that the SSL certificate on the JSS host server is valid and trusted. Choose "Always except during enrollment" if you are using the built-in certificate authority.

Always except during enrollment

Package Validation
Conditions under which to use the checksum to validate packages

When checksum is present

Maximum Clock Skew
Maximum UTC time difference to allow between Mac computers and the JSS host server

No Maximum

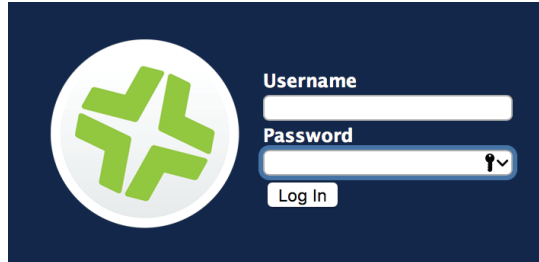
Cancel Save



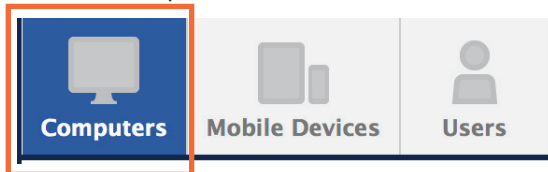
How to Reissue a Recovery Key for Filevault

Section 2 Creating a Configuration Profile

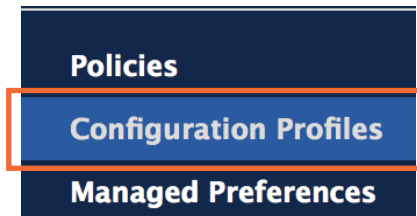
Step 1 Log in to the Jamf Pro Server.



Step 2 Click the Computers button.

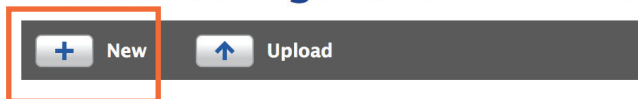


Step 3 Select Configuration Profiles from the left navigation bar.



Step 4 Click the New (+) button.

macOS Configuration Profiles





How to Reissue a Recovery Key for Filevault

Step 5 In the General section, Configure the following:

- Name: Redirect FileVault keys to JSS
- Category: Security (This assumes you have a security category created)
- Distribution Method: Install Automatically
- Level: Computer Level

Options	Scope
General	
Passcode Not Configured	General Name Display name of the profile Redirect FileVault keys to JSS Description Brief explanation of the content or purpose of the profile Category Category to add the profile to Security Distribution Method Method to use for distributing the profile Install Automatically Level Level at which to apply the profile Computer Level
Network Not Configured	
VPN Not Configured	
Certificate Not Configured	
SCEP Not Configured	
Directory Not Configured	
Software Update Not Configured	
Restrictions Not Configured	

Step 6 Select the FileVault Recovery key redirection payload from the left navigation bar (At the bottom). Then click Configure on the right.

Options	Scope
AD Certificate Not Configured	Configure FileVault Recovery Key Redirection Use this section to define settings for FileVault recovery key redirection. Configure
Energy Saver Not Configured	
Custom Settings Not Configured	
Identification Not Configured	
Time Machine Not Configured	
Finder Not Configured	
Accessibility Not Configured	
Proxies Not Configured	
App-to-Per-App VPN Map... Not Configured	
FileVault Recovery Key Red... Not Configured	



How to Reissue a Recovery Key for Filevault

Step 7 Select Automatically, from the Recovery redirection dropdown menu.

Options	Scope
Energy Saver Not Configured	FileVault Recovery Key Redirection Recovery Key Redirection Method to use for specifying the URL to which the recovery keys should be sent Automatically redirect recovery keys to the JSS
Custom Settings Not Configured	
Identification Not Configured	
Time Machine Not Configured	
Finder Not Configured	
Accessibility Not Configured	
Proxies Not Configured	
App-to-Per-App VPN Map... Not Configured	
FileVault Recovery Key Red... 1 Payload Configured	

Step 8 Click on the Scope tab at the top. In the Target Computers dropdown menu, select All Computers.

Options	Scope
Targets Limitations Exclusions	
Target Computers Computers to assign the profile to All Computers	
Target Users Users to distribute the profile to Specific Users	
+ Add	
Target	Type
No Targets	

Step 9 Click the Save button.

Cancel	Save
--------	------

Step 10 Click the Done button.

Done	History	Logs	Download	Clone	Delete	Edit
------	---------	------	----------	-------	--------	------



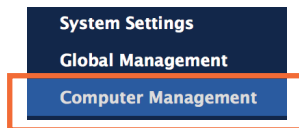
How to Reissue a Recovery Key for Filevault

Section 3 Creating an Extension Attribute

Step 1 On the Jamf Pro Server, click the Settings icon in the upper right corner.



Step 2 Select Computer Management from the left navigation bar.



Step 3 From the Computer Management - Management framework section, select Extension Attributes.

Computer Management - Management Framework



Step 4 Click the New (+) button to Create a new Extension Attribute.

Extension Attributes



Step 5 Configure the following:

- Display Name: FileVault 2 Encryption Check
- Description: This script checks to see if the OS on the Mac is 10.7 or higher and the boot volume was a CoreStorage volume.
- Data Type: String
- Inventory Display: Extension Attribute (This assumes you have a Extension Attribute category created)
- Input Type: Script

a — **Display Name**
Display name for the extension attribute
FileVault 2 Encryption Check

b — **Description**
Description for the extension attribute
This script checks to see if the OS on the Mac is 10.7 or higher and the boot volume was a CoreStorage volume.

c — **Data Type**
Type of data being collected
String


d — **Inventory Display**
Category in which to display the extension attribute in the JSS
Extension Attributes

e — **Input Type**
Input type to use to populate the extension attribute
Script



How to Reissue a Recovery Key for Filevault

Step 6 In the Script section, make sure the macOS tab is selected. Using a plain text editor, like TextWrangler, open Rich Trouton's FileVault status extension attribute: filevault_2_encryption_check_extension_attribute.sh. Copy the contents of the script then paste it into the Script section of the Extension Attribute.

Script 

macOS Windows

Script

Script to use to collect data on Mac computers

```
1 #!/bin/bash
2
3 CORESTORAGESTATUS="/private/tmp/corestorage.txt"
4 ENCRYPTSTATUS="/private/tmp/encrypt_status.txt"
5 ENCRYPTDIRECTION="/private/tmp/encrypt_direction.txt"
6
7 osvers_major=$(sw_vers -productVersion | awk -F. '{print $1}')
8 osvers_minor=$(sw_vers -productVersion | awk -F. '{print $2}')
9
```

Step 7 Click the Save button.




Cancel **Save**

Step 8 Click the Done button.

Done History Download

Step 9 The Extension Attribute is now created and ready for use.

Extension Attributes (1)

 New  New From Template  Upload

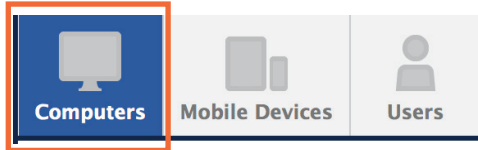
Name
FileVault 2 Encryption Check



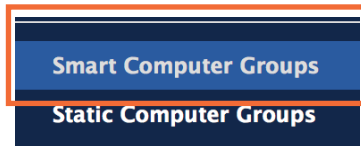
How to Reissue a Recovery Key for Filevault

Section 4 Creating a Smart Group

Step 1 Click the Computers button.



Step 2 Select Smart Computer Groups from the left navigation bar.



Step 3 Click the New (+) button.

Smart Computer Groups

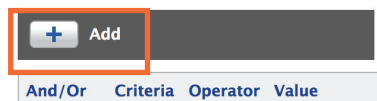


Step 4 Make sure you're on the Computer Group tab, then enter the following:

Display Name: FileVault Encryption Key is Invalid or Unknown

Computer Group	Criteria
Display Name Display name for the smart computer group FileVault Encryption Key is Invalid or Unknc	
<input type="checkbox"/> Send email notification on membership change When group membership changes, send an email notific:	

Step 5 Click the Criteria tab, then click the Add (+) button.



Step 6 Click the Show Advanced Criteria button.

New Criteria	Show Advanced Criteria
Application Title	Choose



How to Reissue a Recovery Key for Filevault

Step 7 Scroll down and locate the FileVault 2 Individual Key Validation and select Choose.

FileVault 2 Individual Key Validation

Choose

Step 8 Configure the following:

- Operator: is not
- Value - Click the Ellipse and choose Valid.

And/Or	Criteria	Operator	Value	
<input type="checkbox"/>	FileVault 2 Individual Key Validation	is not	Valid	<input type="checkbox"/> Delete

a

b

Choice

Invalid

Choose

Unknown

Choose

Valid

Choose

Step 9. Click the Add (+) button.

And/Or	Criteria
<input type="checkbox"/>	FileVault 2 Individual Key Validation

Step 10 Click the Show Advanced Criteria button.

New Criteria	Show Advanced Criteria
Application Title	Choose

Step 11 Scroll down and locate the Last Check-in and select Choose.

Last Check-in	Choose
---------------	--------



How to Reissue a Recovery Key for Filevault

Step 12 Configure the following for Last Check-in:

- Set the And/Or section to: and
- Set the Operator to: less than x days ago
- Set the Value to: 30

And/Or	Criteria	Operator	Value
	FileVault 2 Individual Key Validation	is not	Valid
a	Last Check-in	b	c

Step 13 Click the Add (+) button.

And/Or	Criteria
	FileVault 2 Individual Key Validation
and	Last Check-in

Step 14 Click the Show Advanced Criteria button.

New Criteria
Application Title

Step 15 Scroll down and locate the FileVault 2 Encryption Check and select Choose.

FileVault 2 Encryption Check



How to Reissue a Recovery Key for Filevault

Step 16 Configure the following for FileVault 2 Encryption Check:

- Set the And/Or section to: and
- Set the Operator to: is
- Set the Value to: FileVault 2 Encryption Complete (NOTE: This must be spelled EXACTLY as shown)
- Click the Save button

And/Or	Criteria	Operator	Value	
	FileVault 2 Individual Key Validation	is not	Valid	Delete
and	Last Check-in	less than x days ago	30	Delete
and	FileVault 2 Encryption Check	is	FileVault 2 Encryption Com	Delete

Cancel Save

Step 17 Click the Done button.

Done History View

Step 18 The Smart Computer Group is now created and ready for use.

Smart Computer Groups

+ New

Name

All Managed Clients

All Managed Servers

FileVault Encryption Key is Invalid or Unknown



How to Reissue a Recovery Key for Filevault

Section 5 Configuring the Homebysix Re-Issue Script

Step 1 Open the `reissue_filevault_recovery_key.sh`. Go to the VARIABLES section. This section is what we need to customize to our needs.

```
##### VARIABLES #####

# Your company's logo, in PNG format. (For use in jamfHelper messages.)
# Use standard UNIX path format: /path/to/file.png
LOGO_PNG="/Library/Application Support/HCS/HCSLogo512.png"

# Your company's logo, in ICNS format. (For use in AppleScript messages.)
# Use standard UNIX path format: /path/to/file.icns
LOGO_ICNS="/Library/Application Support/HCS/HCSLogo512.icns"

# The title of the message that will be displayed to the user.
# Not too long, or it'll get clipped.
PROMPT_TITLE="FileVault key repair"

# The body of the message that will be displayed before prompting the user for
# their password. All message strings below can be multiple lines.
PROMPT_MESSAGE="Your Mac's FileVault encryption key needs to be regenerated in order for HCS Technology Group to be able to
recover data from your hard drive in case of emergency.
Click the Next button below, then enter your Mac's password when prompted."

# The body of the message that will be displayed after 5 incorrect passwords.
FORGOT_PW_MESSAGE="You made five incorrect password attempts.
Please contact the the HCS Help Desk at 866.518.9672 for help with your Mac password."

# The body of the message that will be displayed after successful completion.
SUCCESS_MESSAGE="Thank you! HCS key has regenerated your FileVault."
```

Step 2 The LOGO_PNG and LOGO_ICNS paths MUST have a logo in .png and .icns format for this script to work. If you need an app to create your logo in .icns format, You can download this free app, Image2icon, from the App Store:

<https://itunes.apple.com/us/app/image2icon-make-your-own-icons/id992115977?mt=12>

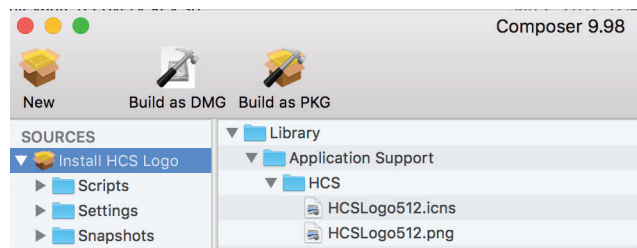
```
# Your company's logo, in PNG format. (For use in jamfHelper messages.)
# Use standard UNIX path format: /path/to/file.png
LOGO_PNG="/Library/Application Support/HCS/HCSLogo512.png"

# Your company's logo, in ICNS format. (For use in AppleScript messages.)
# Use standard UNIX path format: /path/to/file.icns
LOGO_ICNS="/Library/Application Support/HCS/HCSLogo512.icns"
```

Step 3 The .png and .icns files MUST be packaged and installed in the path that you specified in the LOGO_PNG and LOGO_ICNS paths.

I.E. `/Library/Application Support/HCS/HCSLogo512.png`.

You can use Composer to to create a DMG of your files





How to Reissue a Recovery Key for Filevault

Step 4 The rest of the VARIABLES section can be customized to your needs. Save the script when done

```
# The title of the message that will be displayed to the user.
# Not too long, or it'll get clipped.
PROMPT_TITLE="FileVault key repair"

# The body of the message that will be displayed before prompting the user for
# their password. All message strings below can be multiple lines.
PROMPT_MESSAGE="Your Mac's FileVault encryption key needs to be regenerated in order for HCS Technology Group to
    recover data from your hard drive in case of emergency.
Click the Next button below, then enter your Mac's password when prompted."

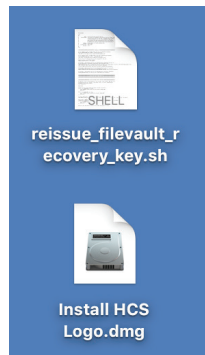
# The body of the message that will be displayed after 5 incorrect passwords.
FORGOT_PW_MESSAGE="You made five incorrect password attempts.
Please contact the the HCS Help Desk at 866.518.9672 for help with your Mac password."

# The body of the message that will be displayed after successful completion.
SUCCESS_MESSAGE="Thank you! HCS key has regenerated your FileVault."
```

Step 5 Launch Casper Admin then upload the reissue_filevault_recovery_key.sh and your DMG or your logos to your Jamf Pro server. Be sure to categorize the script and DMG in Casper Admin.



Casper Admin

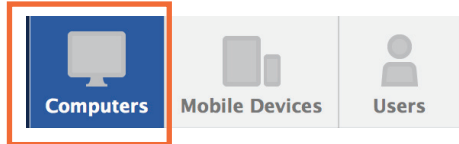




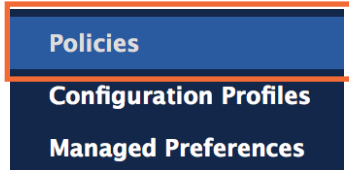
How to Reissue a Recovery Key for Filevault

Section 6 Creating a Policy

Step 1 Click the Computers button

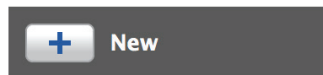


Step 2 Select Policies from the left navigation bar.



Step 3 Click the New (+) button.

Policies (1)



Step 4 Click on the Option tab, then select the General tab on the left.

Configure the following settings:

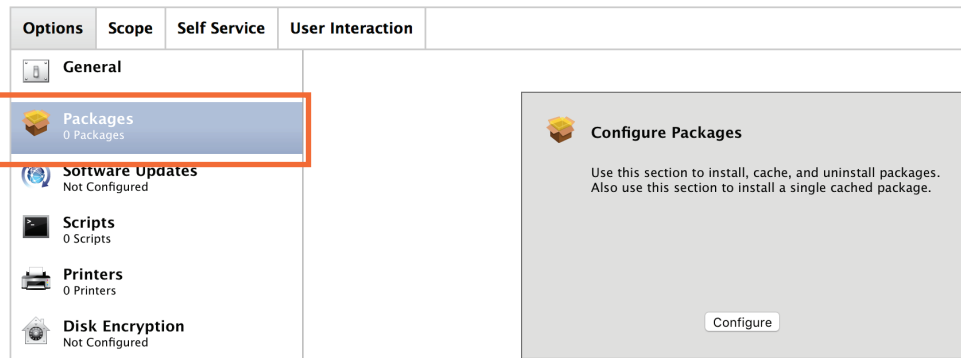
- a. Display Name: Reissue Invalid or missing FileVault recovery key
- b. Category: Security. (This assumes you have a security category created)
- c. Trigger: Recurring Check-in
- d. Execution Frequency- Once per Computer

Options	Scope	Self Service	User Interaction
General			
Display Name Display name for the policy Reissue Invalid or missing FileVault recovery key			
<input checked="" type="checkbox"/> Enabled			
Category Category to add the policy to Security			
Trigger Event(s) to use to initiate the policy <input type="checkbox"/> Startup When a computer starts up. A startup script that ch <input type="checkbox"/> Login When a user logs in to a computer. A login hook th <input type="checkbox"/> Logout When a user logs out of a computer. A logout hook <input type="checkbox"/> Network State Change When a computer's network state changes (e.g. wh when the IP address changes) <input type="checkbox"/> Enrollment Complete Immediately after a computer completes the enrolli <input checked="" type="checkbox"/> Recurring Check-in At the recurring check-in frequency configured in t <input type="checkbox"/> Custom At a custom event			
Execution Frequency Frequency at which to run the policy Once per computer			

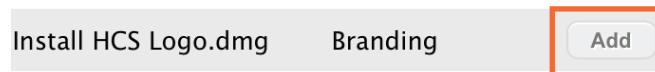


How to Reissue a Recovery Key for Filevault

Step 5 Select Packages from the left navigation bar, then click the Configure button on the right.

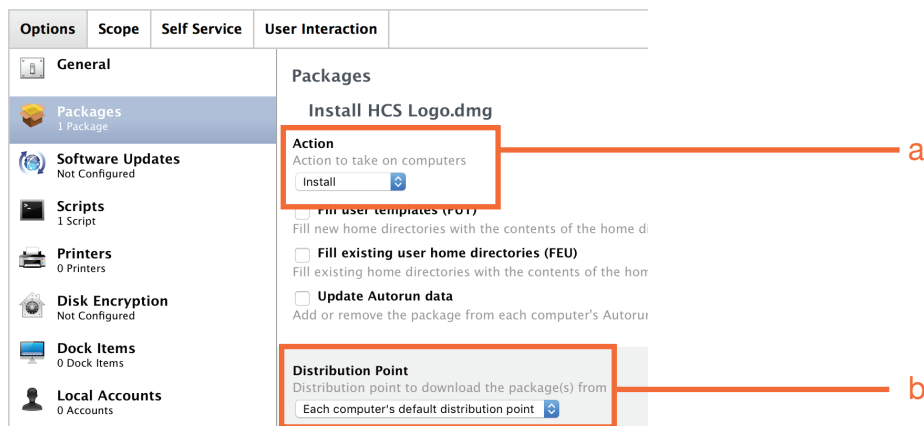


Step 6 Select the DMG of your logo, then click the Add button.

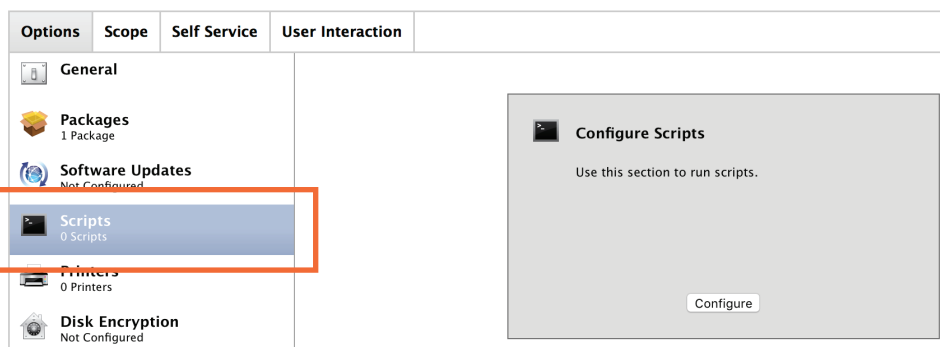


Step 7 Configure the following settings:

- a. Action: Install
- b. Distribution Point: Each computer's default distribution point



Step 8 Select Scripts from the left navigation bar, then click the Configure button on the right.

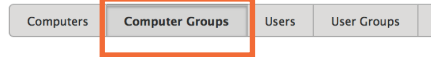




How to Reissue a Recovery Key for Filevault

Step 13 Select the Computer Groups tab, then select FileVault Encryption Key is Invalid or Unknown, then select the Add button.

Add Deployment Targets

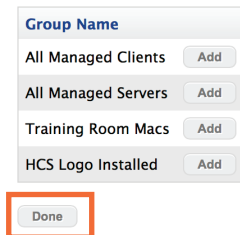


Showing 1 to 5 of 5 entries

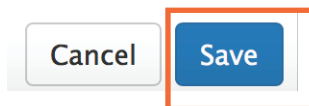


Step 14 Click the Done button.

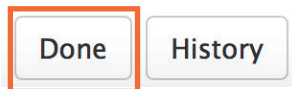
Showing 1 to 5 of 5 entries



Step 15 Click the Save button.

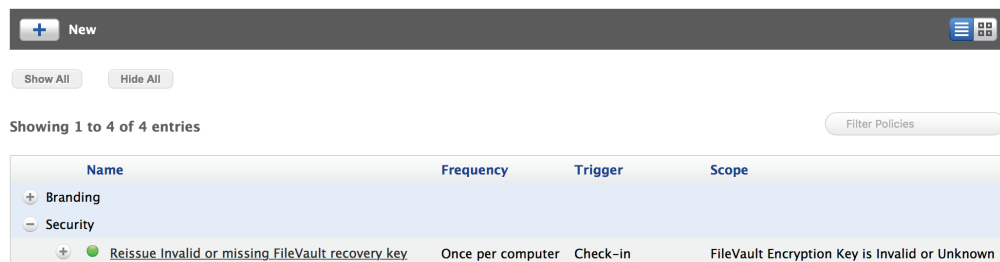


Step 16 Click the Done button.



Step 17 The Policy is now created and ready for use.

Policies (4)





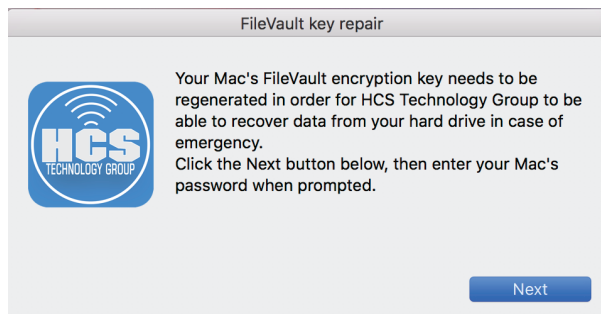
How to Reissue a Recovery Key for Filevault

Section 7 Testing from a Client

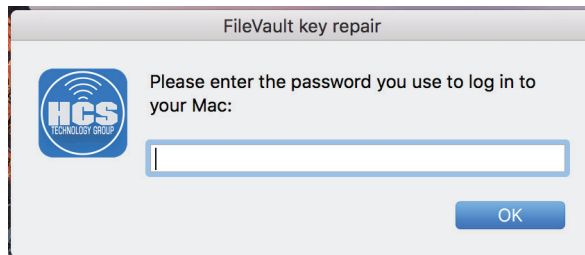
Step 1 Go to a client Mac that already has FileVault enabled but was not escrowed by your Jamf Pro Server. Make sure this Mac is enrolled in your Jamf Pro server. Once enrolled, it will show up in the Smart Computer Group that we created earlier.

Step 2 The next time this client Mac checks into the Jamf Pro server, the currently logged in user will be greeted with the following message:

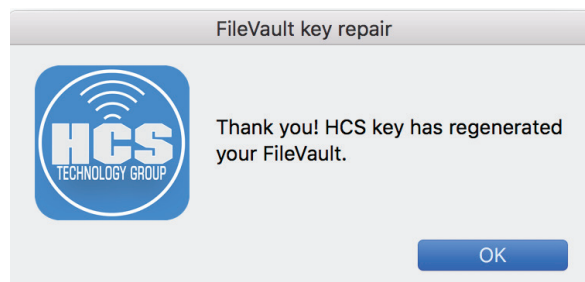
Read the message, then click the Next button



Step 3 The user will be promoted to enter in their login password. Click OK when done.



Step 4 The user will be greeted with the following message. Click OK when done.

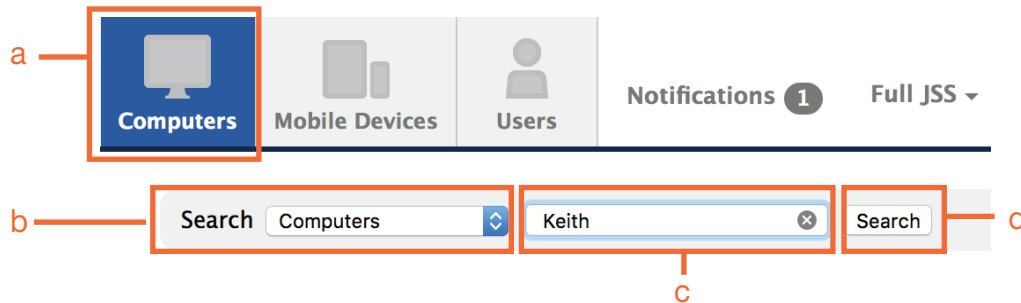




How to Reissue a Recovery Key for Filevault

Step 5 Let's check our work to make sure the FileVault key was escrowed to the Jamf Pro Server

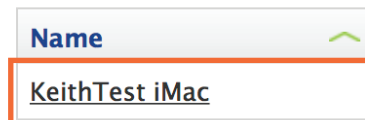
- Click the Computers button.
- In the Search section, Make sure Computers is selected in the drop down menu.
- Enter the computer you want to search for in the Search field.
- Click the Search button.



Step 6 Once the computer is found, click on it's name to view it's computer record.

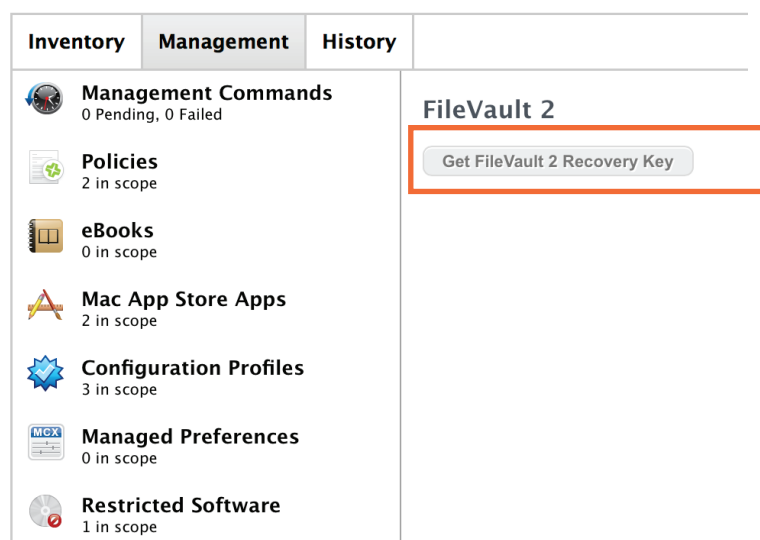
1 Computer

Showing 1 to 1 of 1 entries



Step 7 Once the computer is found, click on it's name to view it's computer record.

KeithTest iMac





How to Reissue a Recovery Key for Filevault

Step 8 You will see the newly escrowed FileVault Key. This completes this how to guide.

KeithTest iMac

Inventory	Management	History
Management Commands 0 Pending, 0 Failed	FileVault 2	
Policies 2 in scope	FileVault 2 Recovery Key: Y4MP-ZLH8-5	
eBooks 0 in scope		
Mac App Store Apps 2 in scope		
Configuration Profiles 3 in scope		
Managed Preferences 0 in scope		
Restricted Software 1 in scope		
FileVault 2 Configured		