

January 27, 2015

Reissuing FileVault Keys with the Casper Suite

Linde Group and the
Pinterest IT Team










MacBrained @ Pinterest — San Francisco, California











The Problem

FileVault recovery keys can be missing from the JSS for many reasons.

- ❖ Perhaps the Mac was encrypted prior to enrollment.
- ❖ The Mac was encrypted without using Casper.
(Using System Preferences or another management framework, for example.)
- ❖ The original recovery key was lost due to a bug in Casper or Mac OS X, or due to database corruption.

The Problem

Inventory	Management	History
	General EX10974	
	Hardware MacBook Air (13-inch Mid 2012)	
	Operating System Mac OS X 10.9.5	
	User and Location	
	Purchasing	
	Storage 1 Drive	
	Extension Attributes	
	Disk Encryption 1 of 1 Partitions Encrypted	
	Licensed Software 1 Match	

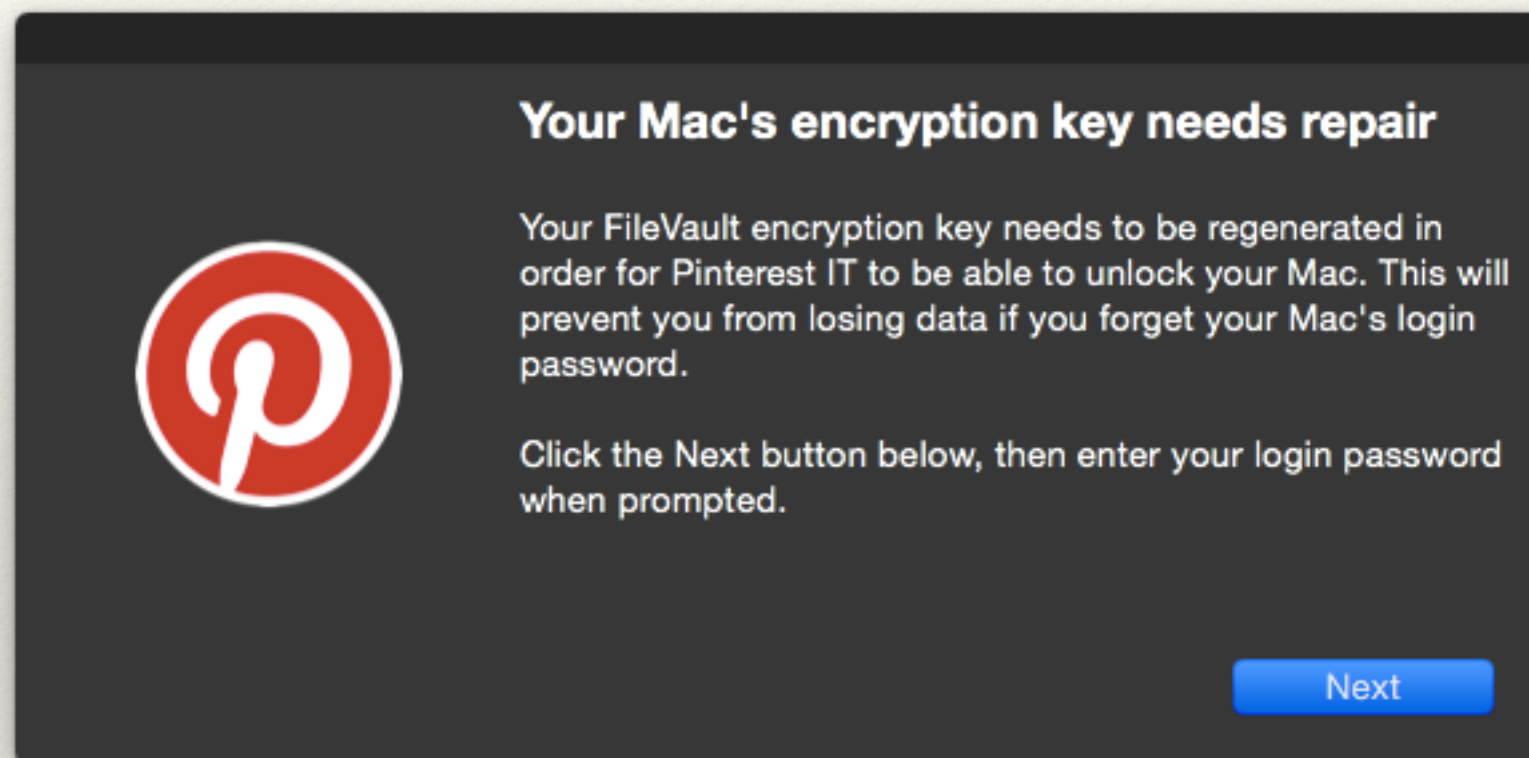
Inventory	Management	History
	Management Commands 0 Pending, 0 Failed	
	Policies 59 in scope	
	eBooks 0 in scope	
	Mac App Store Apps 0 in scope	
	Configuration Profiles 1 in scope	
	Managed Preferences 1 in scope	
	Restricted Software 4 in scope	
	FileVault 2 Not Configured	
	Computer Groups 17 smart, 1 static	

The Solution

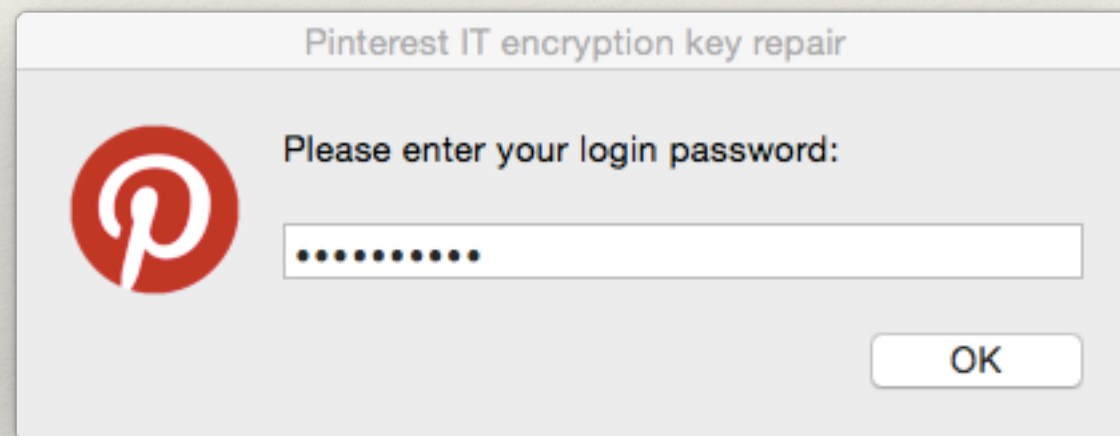
You can use a policy to generate a new FileVault key and upload to JSS.

1. A configuration profile ensures that all FileVault keys are escrowed with the JSS.
2. A smart group determines the computers without valid recovery keys.
3. The reissueKey.sh script can be used as a base, then customized for your environment.
4. A policy deploys the reissueKey.sh script to the computers in the smart group.

The Solution



The Solution



Step One: Configuration Profile

A configuration profile called “Redirect FileVault keys to JSS” does what the name says.

General

- ❖ **Distribution Method: Install Automatically**
- ❖ **Level: Computer Level**

FileVault Recovery Key Redirection

- ❖ **Automatically redirect recovery keys to the JSS**

Scope

- ❖ **All computers**

Step Two: Smart Group

A smart group named “FileVault encryption key is invalid or unknown” selects the affected Macs.

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

* From Rich Trouton's FileVault status extension attribute: <http://goo.gl/zB04LT>

Step Three: **Script**

A customized version of JAMF's reissueKey.sh script runs on each affected Mac.

- ❖ Start by making a local copy of reissueKey.sh: <http://goo.gl/e9HXr3>
- ❖ Customize as needed for your environment. Here's what we tailored to Pinterest:
 - ❖ **Emailed** affected employees to give them a heads up.
 - ❖ Use **jamfHelper** to announce the upcoming password prompt.
 - ❖ Add **logo** to AppleScript password prompt.
 - ❖ **Fail silently** if logo files aren't present, or any other problems detected.
 - ❖ **Verification** of the Mac login password, with 5 chances to enter correct password.

Step Three: Script

1. Explain the prompt that's about to appear.

2. Show the branded password prompt.

3. Show it again if the password was incorrect.

4. Success!

```
# Display a Pinterest-branded prompt explaining the password prompt.
"$jamfHelper" -windowType hud -lockHUD -icon "$LOGO" -heading "$PROMPT_HEADING"
-description "$PROMPT_MESSAGE" -button1 "Next" -defaultButton 1

## Get the logged in user's password via a prompt
echo "Prompting ${userName} for their Mac password (try 0)..."
userPass="$(/usr/bin/osascript -e 'tell application "System Events" to display
dialog "Please enter your Mac password:" default answer "" with title
"Pinterest IT encryption key repair" with text buttons {"OK"} default
button 1 with hidden answer with icon file "private:tmp:Pinterest.icns" -e
'text returned of result')'"

TRY=0
until dscl /Search -authonly "$userName" "$userPass" &> /dev/null; do
    let TRY++
    echo "Prompting ${userName} for their Mac password (try $TRY)..."
    userPass="$(/usr/bin/osascript -e 'tell application "System Events" to
display dialog "Sorry, that password was incorrect. Please try again:"
default answer "" with title "Pinterest IT encryption key repair" with
text buttons {"OK"} default button 1 with hidden answer with icon file
"private:tmp:Pinterest.icns" -e 'text returned of result')'"
    if [[ $TRY -ge 4 ]]; then
        echo "Password prompt unsuccessful after 5 attempts."
        exit 1007
    fi
done
echo "Successfully prompted for Mac password."
```

Step Four: Policy

A policy called “Reissue invalid or missing FileVault recovery key” runs the script on each Mac in the smart group.

General

- ❖ Trigger: **Recurring Check-In**
- ❖ Execution Frequency: **Once per computer**

Packages

- ❖ **AppleScriptCustomIcon.dmg** (loads */tmp/Pinterest.icns*)

Scripts

- ❖ **pinterest_reissue_filevault_recovery_key.sh** (priority: **After**)

Scope

- ❖ Smart Group: **FileVault encryption key is invalid or unknown**

Follow Through

Don't forget to monitor policy logs and test FileVault recovery to verify success.

- ❖ Monitor logs and flush one-off errors.
(Unable to connect to distribution point, no user logged in, etc.)
- ❖ Identify and resolve remaining problems manually.
- ❖ Test a few newly-generated FileVault keys to ensure they are working as expected.
- ❖ Update your internal documentation.
(No, pasting a link to these slides does not count.)

Thank you!

Elliot Jordan

elliot@lindegroupp.com

Download these slides: <http://goo.gl/fbojly>

