



How to Configure Escrow Buddy  
to Escrow a FileVault Personal Recovery Key  
(PRK) in Jamf Pro



## Contents

Preface.....	3
Section 1: Configure Jamf Pro.....	4
Section 2: FileVault personal recovery key (PRK) escrow with Escrow Buddy.....	16
Section 3: Ensuring persistent escrow of the FileVault key.....	22

## Preface

### What is Escrow Buddy?

Escrow Buddy was created to ensure a valid FileVault personal recovery key (PRK) is escrowed to and MDM server. There are many reasons recovery keys can be missing from your MDM server:

- Prior to MDM enrollment, FileVault may have been enabled.
- The absence of the MDM escrow payload on the Mac could be due to scoping issues or misconfiguration in your MDM settings.
- The Mac computers might be in the process of transitioning from a different MDM system where the FileVault keys are currently escrowed.
- The integrity of your escrowed keys may have been compromised due to MDM database corruption or instances of data loss.

Escrow Buddy's authorization plugin is crafted to create a new key when a user logs in to macOS. It achieves this by using the user's login credentials as input for the `fdesetup` tool. This seamless integration with the macOS login window eliminates the need to show additional prompts or on-screen messages to the user.

Regardless of how FileVault was enabled on your Mac, Escrow Buddy will create a new FileVault recovery key and escrow it your MDM server provided your MDM server is deploying a **`FDERecoveryKeyEscrow`** Payload to your managed Macs. This guide will walk you through the steps for deploying and configuring Escrow Buddy using Jamf Pro as the MDM server.

Requirements:

- An MDM server that supports the following:
  - FileVault recovery key escrow
  - Install Packages
  - Run Shell Scripts
  - Deploy a configuration profile with the **`FDERecoveryKeyEscrow`** payload
- A Mac with macOS Mojave 10.14.4 or later and enrolled in your MDM server

NOTE: Escrow Buddy only works with MDM-based escrow solutions, not escrow servers like Crypt Server or Cauliflower Vest.

A very special thanks to Elliot Jordan and the Netflix client systems engineering team for making Escrow Buddy available to the Mac community. Be sure to check out the Escrow Buddy Wiki for future updates and workflow options for Jamf Pro.

<https://github.com/macadmins/escrow-buddy/wiki/Jamf>

This guide was written using the following:

- macOS Ventura 13.4.1
- Jamf Pro server version 10.48
- Escrow Buddy version 1.0.0



## Section 1: Configure Jamf Pro

### What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

### Hardware and Software

Requirements for following along with this section:

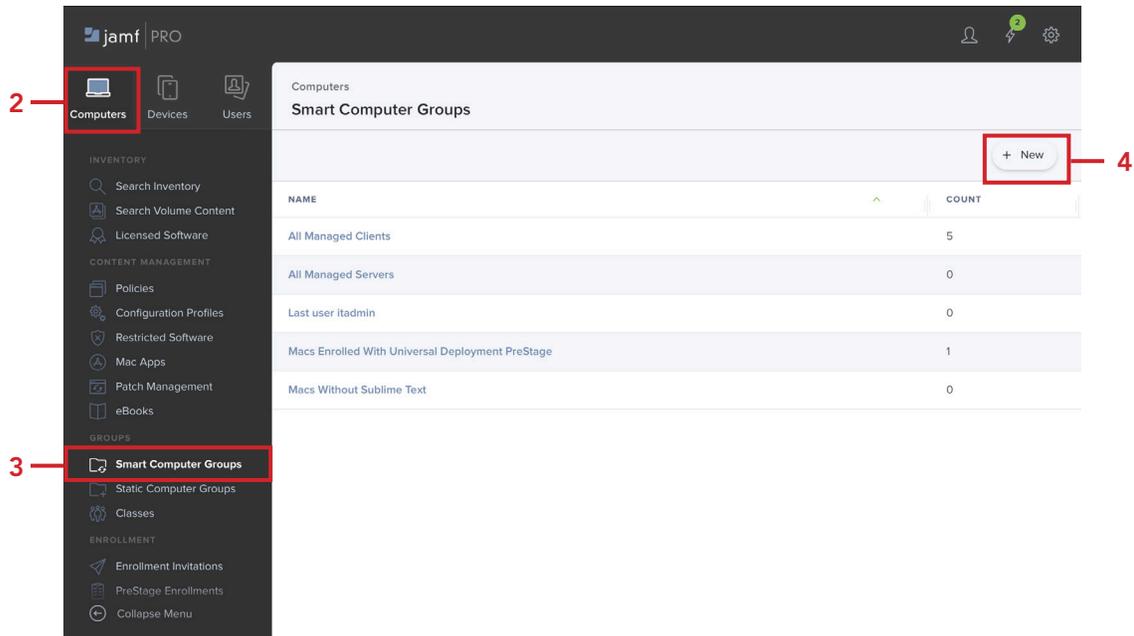
- Jamf Pro server that supports the FDERecoveryKeyEscrow payload. This guide will use version 10.48
- Jamf Pro administrator credentials
- Escrow Buddy version 1.0.0 or later.

<https://github.com/macadmins/escrow-buddy/releases/latest>

1. Log into your Jamf Pro server with administrative credentials.



2. Click Computers
3. Click Smart Computer Groups.
4. Click New.





5. Configure the following:

- A. Enter for Display Name: **FileVault Encryption Key is Invalid or Unknown**
- B. Configure other items to your need. This guide will leave them at their defaults.
- C. Click Criteria

Computers : Smart Computer Groups  
← **New Smart Computer Group**

Computer Group Criteria

**Display Name** Display name for the smart computer group  
FileVault Encryption Key is Invalid or Unknown

Send email notification on membership change  
When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

6. Click Add.

Computers : Smart Computer Groups  
← **New Smart Computer Group**

Computer Group Criteria

AND/OR	CRITERIA	OPERATOR	VALUE
--------	----------	----------	-------

+ Add

7. Configure the following for the Criteria as shown below:

- A. Criteria: **FileVault 2 Individual Key Validation**
- B. Operator: **is**
- C. Value: **Invalid**
- D. Click Add

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE
	FileVault 2 Individual Key Validation	is	Invalid

+ Add

8. Configure the following for the Criteria as shown below:

- A. Criteria: **FileVault 2 Individual Key Validation**
- B. And/Or: **or**
- C. Operator: **is**
- D. Value: **Unknown**
- E. Click Add

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE
	FileVault 2 Individual Key Validation	is	Invalid
or	FileVault 2 Individual Key Validation	is	Unknown

+ Add



9. Configure the following for the Criteria as shown below:

A. Criteria: **FileVault 2 Partition Encryption State**

B. And/Or: **and**

C. Operator: **is**

D. Value: **Encrypted**

E. Click Save

AND/OR	CRITERIA	OPERATOR	VALUE	
	FileVault 2 Individual Key Validation	is	Invalid	Delete
or	FileVault 2 Individual Key Validation	is	Unknown	Delete
and	FileVault 2 Partition Encryption State	is	Encrypted	Delete

Buttons: + Add, Cancel, Save

10. Select the checkbox for Show in Jamf Pro Dashboard.

NOTE: We created this smart group to use for scoping later on in this guide.

Computers : Smart Computer Groups

← FileVault Encryption Key is Invalid or Unknown

Computer Group Criteria Reports

Show in Jamf Pro Dashboard

11. Click Computers.

12. Click Configuration Profiles.

13. Click New.

jamf PRO

Computers Configuration Profiles

11 Computers 12 Configuration Profiles 13 + New

Filter Pr 1-32 of 32

NAME LOGS COMPLETED PENDING FAILED SCOPE



- Click the General payload and enter the following:
  - Name: **FileVault Key Escrow**
  - Description: Add a description of your choosing if needed.
  - Category: This guide will use Security. Feel free to select a category of your choosing.
  - Leave all other items at their default settings.

Options Scope

Search...

General

Accessibility Not configured

AD Certificate Not configured

AirPlay Not configured

App-To-Per-App VPN Mapping Not configured

Application & Custom

**General**

Name Display name of the profile  
FileVault Key Escrow **A**

Description Brief explanation of the content or purpose of the profile  
**B**

Site Site to add the profile to  
None

Category Category to add the profile to  
Security **C**

Level Level at which to apply the profile  
Computer Level

- Scroll down and click Security and Privacy payload
- Click FileVault.
- Configure the following:
  - Enable FileVault: **Enable**
  - Scroll down to Escrow Personal Recovery Key.

Computers : Configuration Profiles

← New macOS Configuration Profile

Options Scope

Search...

Printing Not configured

Privacy Preferences Policy Control Not configured

Proxies Not configured

Restrictions Not configured

SCEP Not configured

**Security and Privacy** Settings configured: 4

General

FileVault

Firewall

Single Sign-On Extensions Not configured

**Security and Privacy: FileVault** Settings configured: 4

Exclude all

Include **17A**

**Setting**

**Enable FileVault**  
FileVault provides full disk encryption to the macOS boot volume. User Approved MDM required for macOS 10.15 or later

**Event to prompt FileVault enablement**  
Specify when macOS prompts the user to enable FileVault. Only users with a SecureToken can enable FileVault on computers with the APFS boot volumes.  
At Logout At Login

**Allow users to bypass FileVault prompts at login**  
Maximum number of times users can bypass enabling FileVault before being required to enable it to log in  
Require on the next login

**Recovery keys**  
Enable access to the encrypted drive using a recovery key  
Personal Recovery Key

**Display personal recovery key to user**  
If hidden, prevents the personal recovery key from being displayed to the end user after FileVault is enabled  
Hide Display

**User adjustment of FileVault options**  
Prevent end user from enabling or disabling FileVault  
Prevent FileVault from being disabled

Required settings applied due to Enable FileVault dependency



- 18. Configure the following:
  - A. Escrow Personal Recovery Key: **Enable**
  - B. Encryption Method: **Automatically encrypt and decrypt recovery key.**
  - C. Escrow Location: **Jamf Pro Server.**
  - D. Click Scope.

The screenshot shows the 'New macOS Configuration Profile' page in Jamf Pro. The 'Scope' tab is selected, indicated by a red box and label 'D'. The 'Escrow Personal Recovery Key' section has a toggle switch turned on, labeled 'A'. The 'Encryption Method' dropdown is set to 'Automatically encrypt and decrypt recovery key', labeled 'B'. The 'Escrow Location Description' section has 'Jamf Pro Server' entered in the text field, labeled 'C'. The left sidebar shows various configuration categories like Printing, Privacy Preferences Policy, Proxies, Restrictions, and SCEP.

- 19. Click Targets
- 20. Confirm Specific Computers is selected for Target Computers.
- 21. Click Add

The screenshot shows the 'New macOS Configuration Profile' page in Jamf Pro, specifically the 'Targets' section. The 'Targets' tab is selected, indicated by a red box and label '19'. The 'Target Computers' dropdown menu is set to 'Specific Computers', labeled '20'. The 'Target Users' dropdown menu is set to 'Specific Users'. The 'Selected Deployment Targets' table is empty, and the '+ Add' button is highlighted with a red box and label '21'.



22. Click Computer Groups.
23. Click Add for "FileVault Encryption Key is Invalid or Unknown."
24. Click Save.

Computers : Configuration Profiles  
← FileVault Key Escrow

Options Scope

Targets Limitations Exclusions

Add Deployment Targets Done

Computers Computer Groups Users User Groups Buildings Departments

Filter Re 1-7 of 7

GROUP NAME	
All Managed Clients	Add
Macs Without Sublime Text	Add
Last user itadmin	Add
Filardo	Add
FileVault Encryption Key is Invalid or Unknown	Add
All Managed Servers	Add
Macs Enrolled With Universal Deployment PreStage	Add

Show: 1

Cancel Save

25. Download Escrow Buddy.  
<https://github.com/macadmins/escrow-buddy/releases/latest>

macadmins / escrow-buddy Public

Notifications Fork 2 Star 85

Code Issues Pull requests Actions Wiki Security Insights

Releases / v1.0.0

Escrow Buddy 1.0.0 Latest

homebysix released this Jun 12 · 2 commits to main since this release v1.0.0 d176770

Initial public release of Escrow Buddy!

See the announcement on the Netflix Tech Blog, and refer to the readme and wiki for documentation.

Assets 3

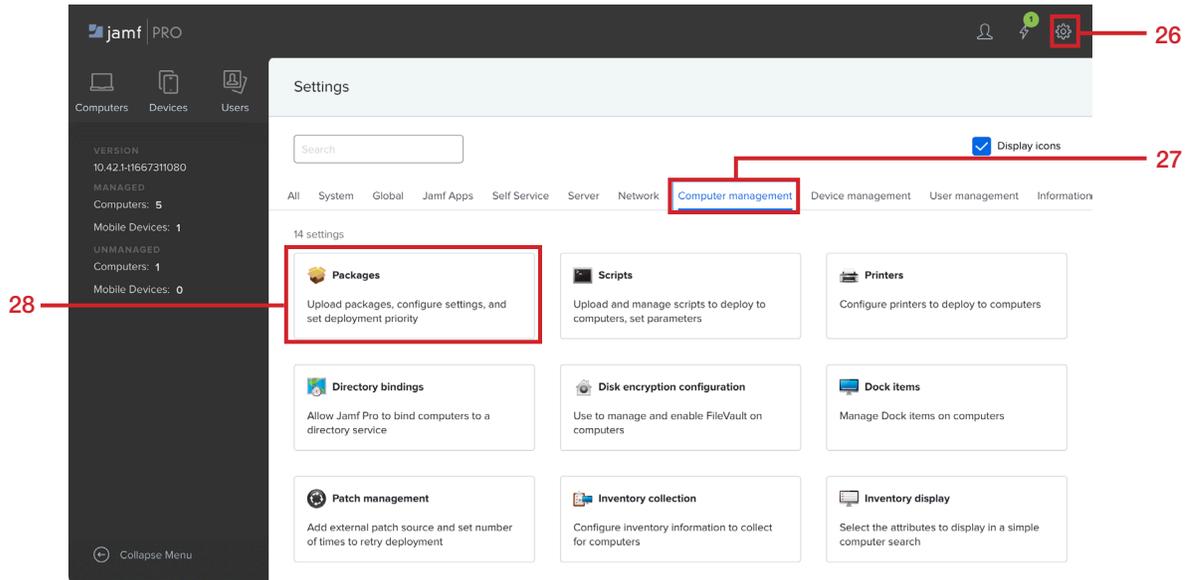
Escrow.Buddy-1.0.0.pkg	82 KB	Jun 11
Source code (zip)		Jun 11
Source code (tar.gz)		Jun 11



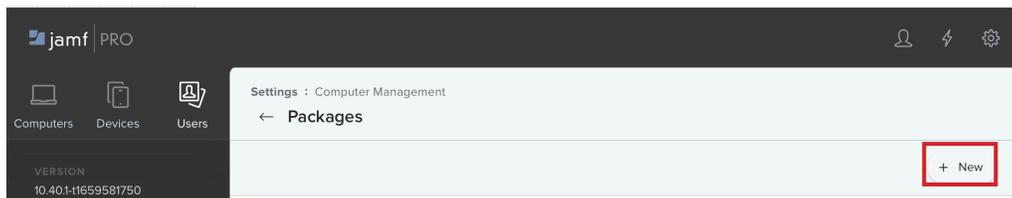
26. Switch back to your Jamf Pro Server instance. On the top-right corner, click Settings (⚙️).

27. Click Computer management.

28. Click Packages.



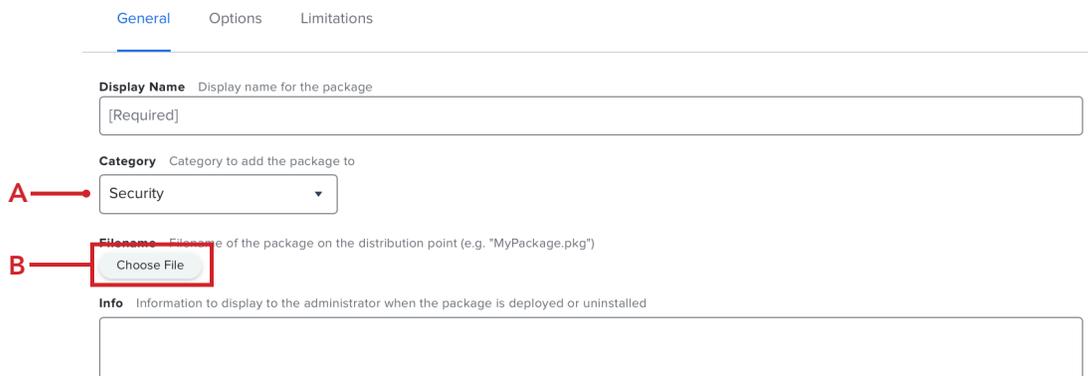
29. Click New.



30. Configure the following:

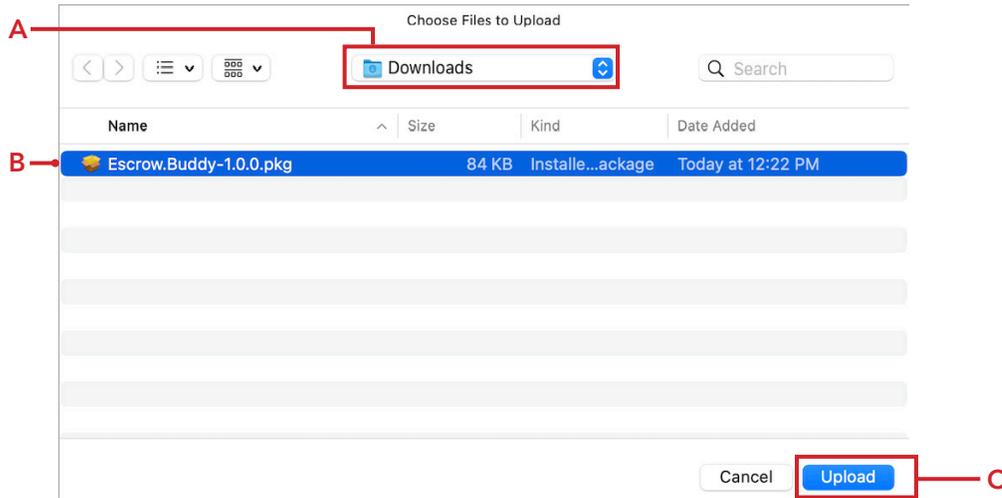
A. Category: This guide will use Security

B. Click Choose File

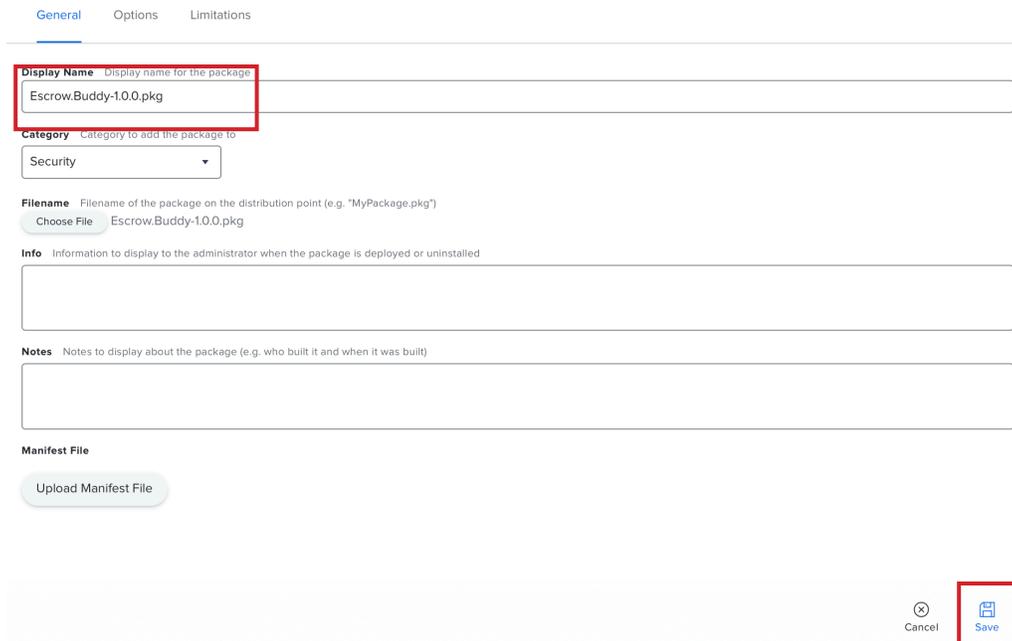




30. Perform the following:
- A. Navigate to your Downloads folder
  - B. Select Escrow.Buddy-1.0.0.pkg
  - C. Click Upload

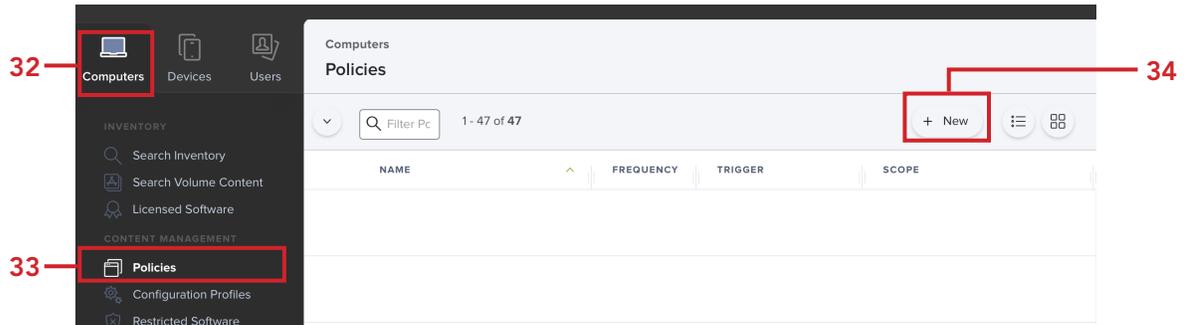


31. Confirm the Display Name auto-populates with the name Escrow.Buddy-1.0.0.pkg. Click Save.

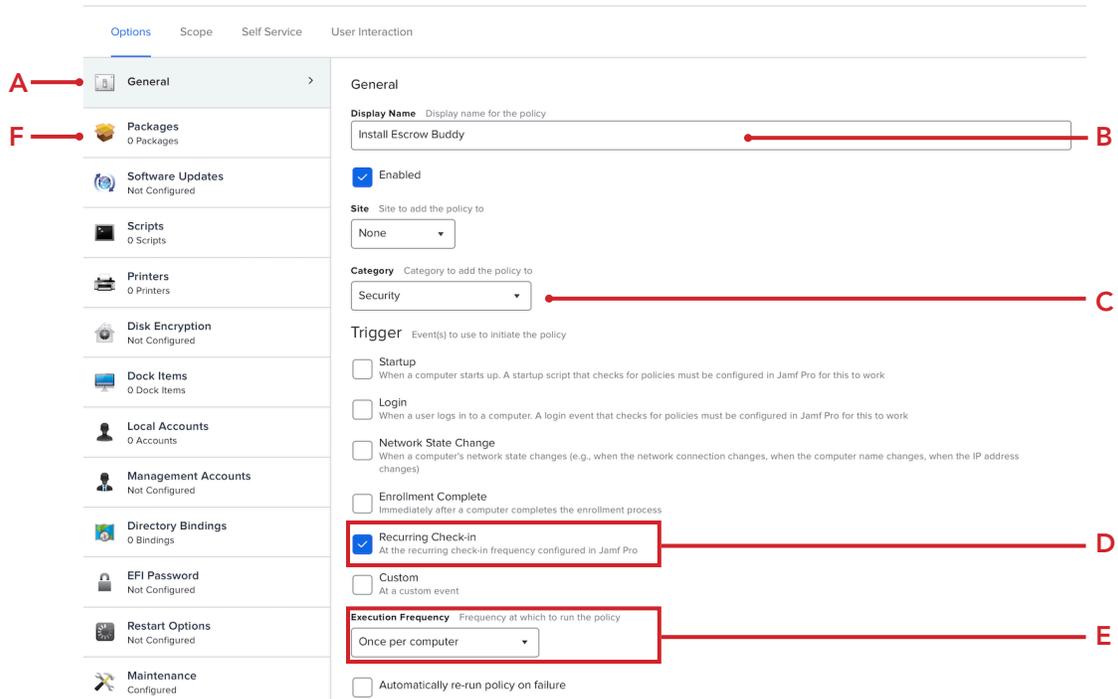




- 32. Click Computers.
- 33. Click Policies.
- 34. Click New.

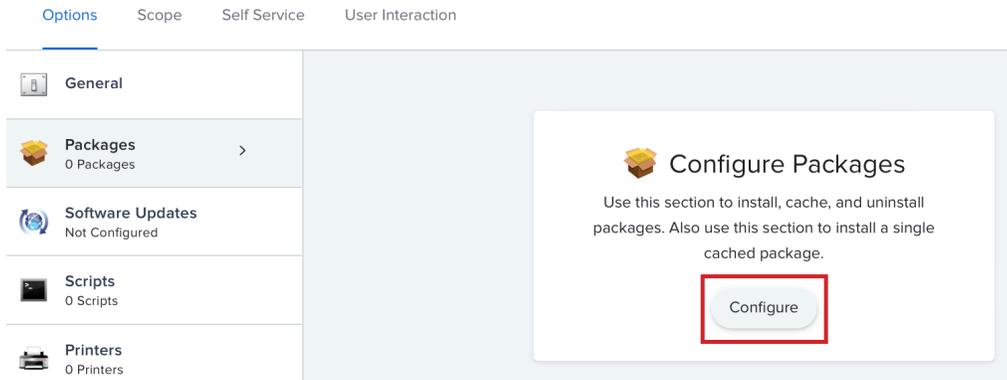


- 35. Configure the following:
  - A. Click General
  - B. Display Name: **Install Escrow Buddy**
  - C. Category: **Security**
  - D. Trigger: **Recurring Check-in**
  - E. Execution Frequency: **Once per computer**
  - F. Click Packages





36. Click Configure.



37. Click Add for Escrow.Buddy-1.0.0.pkg.

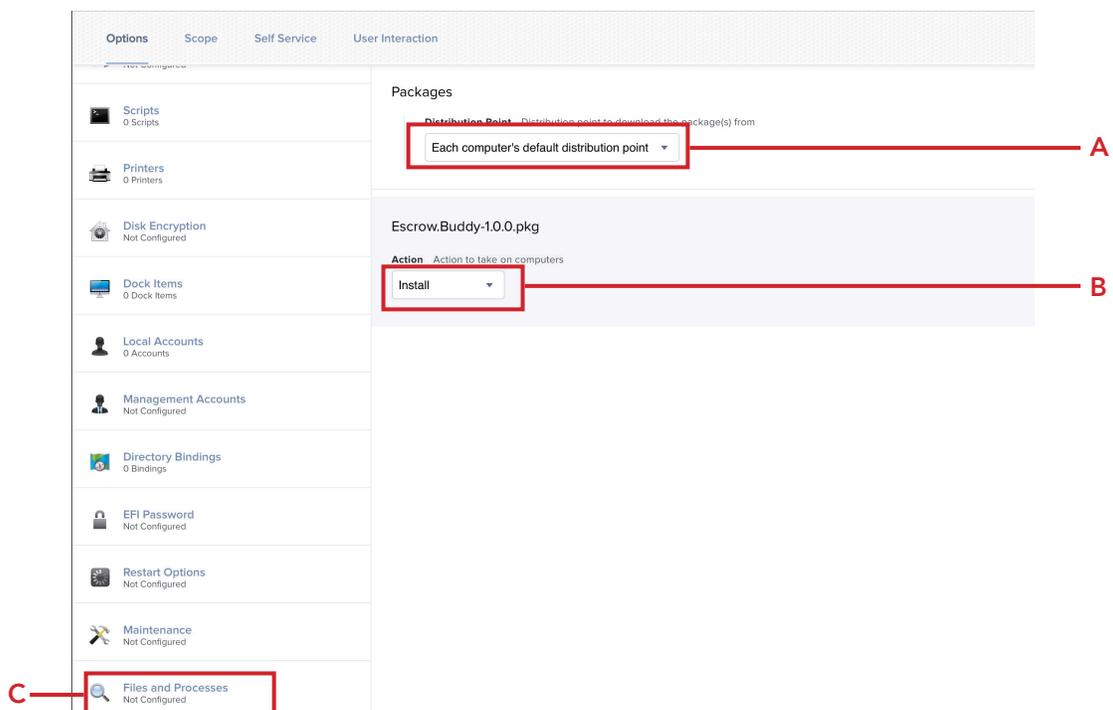


38. Confirm the following:

A. Distribution Point: This guide will use the default shown below.

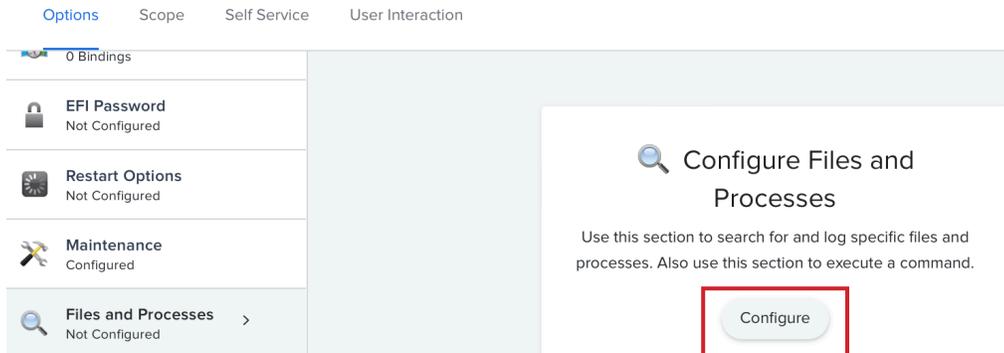
B. Action: **Install**

C. Scroll Down and click Files and Processes payload.





39. Click Configure.

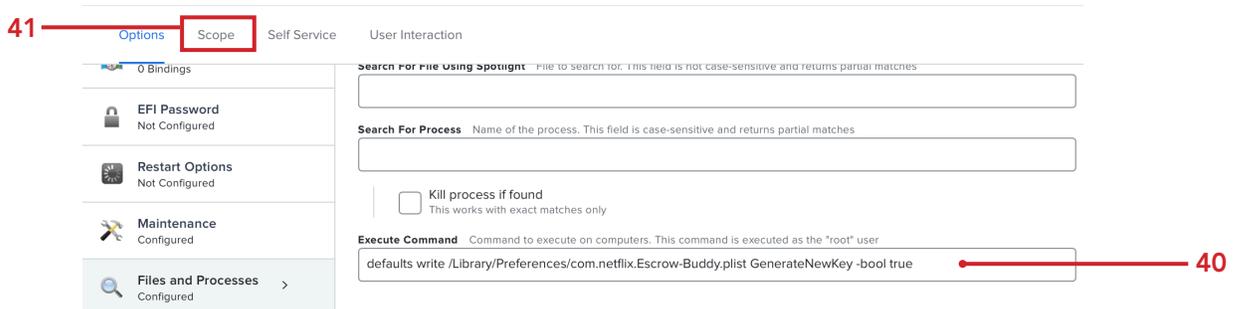


40. In the Execute Command field, enter the following:

```
defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true
```

Note: The defaults command configures Escrow Buddy to regenerate a key upon next login.

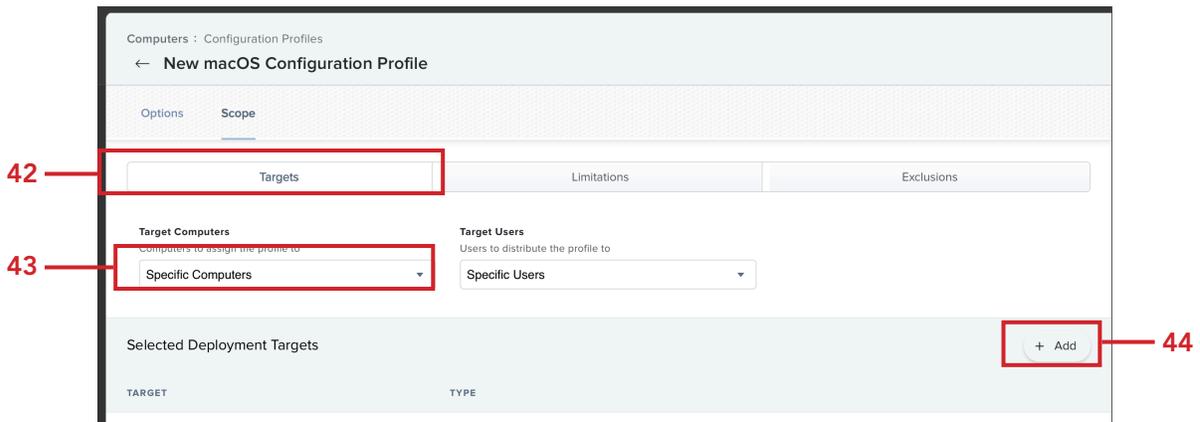
41. Click Scope.



42. Click Targets

43. Confirm Specific Computers is selected for Target Computers.

44. Click Add





- 45. Click Computer Groups.
- 46. Click Add for "FileVault Encryption Key is Invalid or Unknown."
- 47. Click Save.

Computers : Configuration Profiles  
← FileVault Key Escrow

Options Scope

Targets Limitations Exclusions

Add Deployment Targets Done

Computers Computer Groups Users User Groups Buildings Departments

Filter Re 1 - 7 of 7

GROUP NAME	
All Managed Clients	Add
Macs Without Sublime Text	Add
Last user itadmin	Add
Filardo	Add
FileVault Encryption Key is Invalid or Unknown	Add
All Managed Servers	Add
Macs Enrolled With Universal Deployment PreStage	Add

Show: 1

Cancel Save

This completes this section. In the next section, we will enroll a Mac computer that is already FileVault encrypted into our Jamf Pro server to see how Escrow Buddy can re-key and escrow it back to the Jamf Pro server without prompting the user.



## Section 2: FileVault personal recovery key (PRK) escrow with Escrow Buddy

### What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

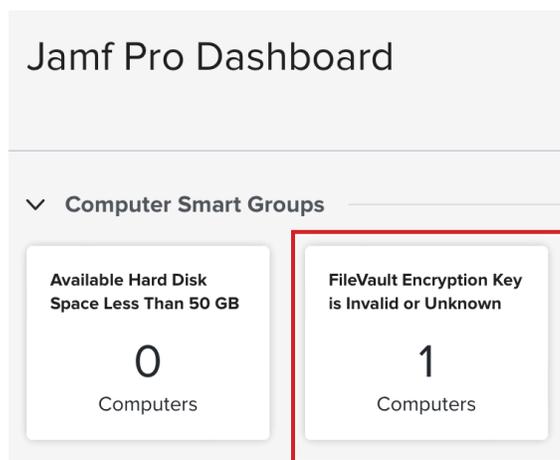
### Hardware and Software

Requirements for following along with this section:

- A Mac with macOS Mojave 10.14.4 or later with FileVault enabled and NOT enrolled in Jamf Pro.
  - Jamf Pro administrator credentials
1. Enroll your Mac computer into the Jamf Pro server. This can be done via User Initiated Enrollment or an Enrollment Invitation email if SMTP is configured on your Jamf Pro server.
  2. Log into your Jamf Pro Server.

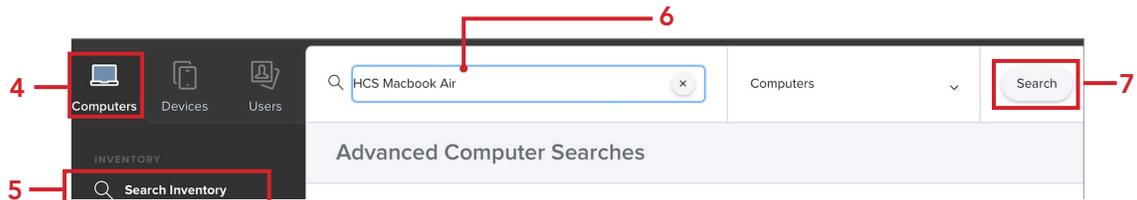


3. The Jamf Pro Dashboard should show at least one computer in the "FileVault Encryption Key is Invalid or Unknown" Smart Computer Group.

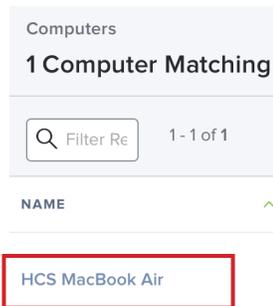




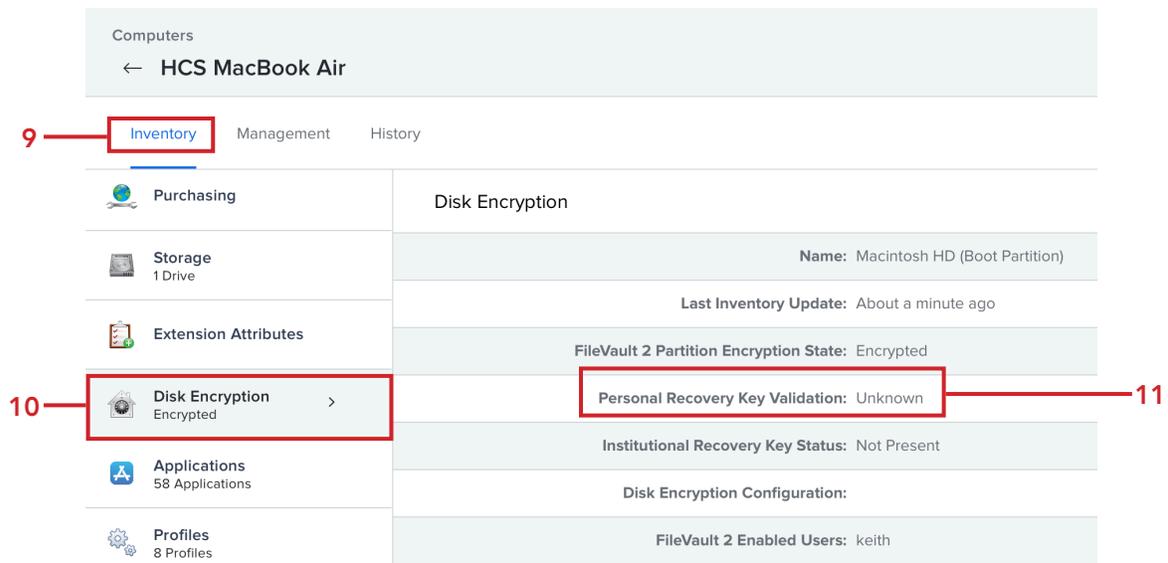
4. Click Computers.
5. Click Search Inventory
6. In the search field, enter the name of the computer you just enrolled
7. Click Search



8. Click on your Mac computer.



9. Click Inventory.
10. Click Disk Encryption.
11. Verify the Personal Recovery Key Validation is Unknown.





12. Open Terminal.



Terminal

13. Depending on the check in time set on your Jamf Pro server, it could take a while for the Escrow Buddy policy to run. We will use the commands below to run the policy immediately and update the inventory.

**sudo jamf policy**

Enter your administrator password when prompted.

```
keith — zsh — 149x34
Last login: Sun Jul 16 15:02:47 on ttys000
keith@keiths-Air ~ % sudo jamf policy
Password:
Checking for policies triggered by "recurring check-in" for user "keith"...
Executing Policy Install Escrow Buddy
Downloading Escrow.Buddy-1.0.0.pkg...
Downloading https://use1-jcfs.services.jamfcloud.com/download/4d31cf5119844ef69281760d82c46a16/Escrow.Buddy-1.0.0.pkg...
Verifying package integrity...
Installing Escrow.Buddy-1.0.0.pkg...
Successfully installed Escrow.Buddy-1.0.0.pkg.
Running command defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true...
Result of command:

Checking for patches...
No patch policies were found.
Running Recon...
Retrieving inventory preferences from https://jamfcloud.com/...
Finding extension attributes...
Locating applications...
Locating package receipts...
Searching path: /System/Applications
Locating hard drive information...
Locating accounts...
Gathering application usage information from the JamfDaemon...
Searching path: /Applications
Locating hardware information (macOS 13.4.1)...
Submitting data to https://jamfcloud.com/...
<computer_id>189</computer_id>
Submitting log to https://jamfcloud.com/
keith@keiths-Air ~ %
```

14. Enter the command below to ensure the inventory is updated on the Jamf Pro server.

**sudo jamf recon**

Enter your administrator password if required.

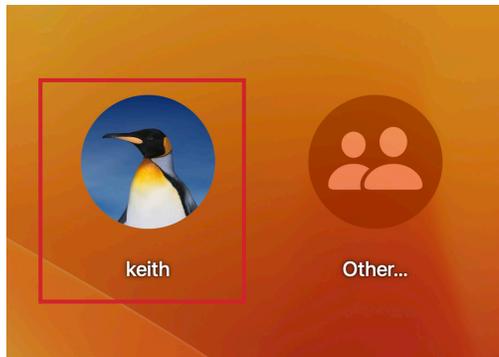
```
keith — zsh — 90x29
Last login: Sun Jul 16 15:11:34 on console
keith@hcs-macbook-air ~ % sudo jamf recon
Password:
Retrieving inventory preferences from https://jamfcloud.com/...
Finding extension attributes...
Locating accounts...
Locating package receipts...
Locating hard drive information...
Locating applications...
Searching path: /System/Applications
Gathering application usage information from the JamfDaemon...
Searching path: /Applications
Locating hardware information (macOS 13.4.1)...
Submitting data to https://jamfcloud.com/...
<computer_id>189</computer_id>
keith@hcs-macbook-air ~ %
```



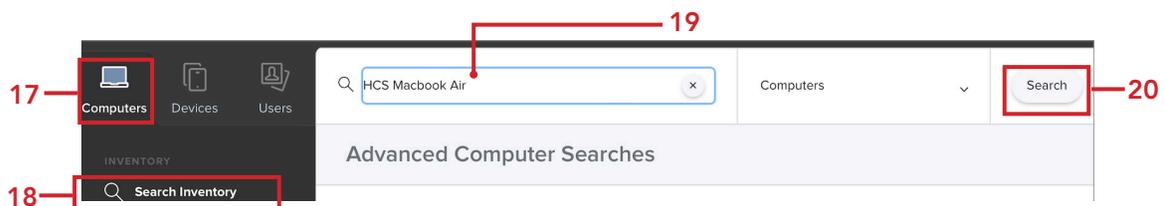
15. Log out of your Mac computer.



16. Log back into your Mac computer. Escrow Buddy will initiate the FileVault Re-Key and escrow the key in the Jamf Pro server.



- 17. Switch back to your Jamf Pro server. Click Computers
- 18. Click Search Inventory
- 19. In the search field, enter the name of the computer you just enrolled
- 20. Click Search





21. Select your Mac computer.

Computers  
**1 Computer Matching**

Filter Re 1 - 1 of 1

NAME ^

HCS MacBook Air

22. Click Inventory.

23. Click Disk Encryption.

24. Verify the Personal Recovery Key and the Device Recovery Key both have Show Key buttons.

← HCS MacBook Air

**22** — [Inventory](#) Management History

<b>General</b> HCS MacBook Air	<b>Disk Encryption</b>
<b>Hardware</b> MacBook Air (M2, 2022)	Name: Macintosh HD (Boot Partition)
<b>Operating System</b> macOS 13.4.1	Last Inventory Update: 15 minutes ago
<b>User and Location</b>	FileVault 2 Partition Encryption State: Encrypted
<b>Security</b>	Personal Recovery Key Validation: Valid
<b>Purchasing</b>	Personal Recovery Key <input type="button" value="Show Key"/>
<b>Storage</b> 1 Drive	Device Recovery Key <input type="button" value="Show Key"/>
<b>Extension Attributes</b>	Institutional Recovery Key Status: Not Present
<b>23</b> — <b>Disk Encryption</b> Encrypted >	Disk Encryption Configuration: FileVault 2 Enabled Users: keith

**24** —



25. Click Show Key on Personal Recovery Key and Device Recovery Key to display the keys.

Computers

← HCS MacBook Air

Inventory Management History

<b>General</b> HCS MacBook Air	<b>Disk Encryption</b>
<b>Hardware</b> MacBook Air (M2, 2022)	<b>Name:</b> Macintosh HD (Boot Partition)
<b>Operating System</b> macOS 13.4.1	<b>Last Inventory Update:</b> 16 minutes ago
<b>User and Location</b>	<b>FileVault 2 Partition Encryption State:</b> Encrypted
<b>Security</b>	<b>Personal Recovery Key Validation:</b> Valid
<b>Purchasing</b>	<b>Personal Recovery Key:</b> I [REDACTED] K
<b>Storage</b> 1 Drive	<b>Device Recovery Key:</b> C [REDACTED]
<b>Extension Attributes</b>	<b>Institutional Recovery Key Status:</b> Not Present
<b>Disk Encryption</b> Encrypted >	<b>Disk Encryption Configuration:</b>
	<b>FileVault 2 Enabled Users:</b> keith

The FileVault keys are now escrowed on the Jamf Pro server.



## Section 3: Ensuring persistent escrow of the FileVault key

### What You'll Need

Learn what hardware, software, and information you'll need to complete the tutorials in this section.

### Hardware and Software

Requirements for following along with this section:

- Jamf Pro administrator credentials

At times, a newly generated FileVault Personal Recovery Key (PRK) may initially appear valid on the Jamf Pro server but later become invalid or go missing. While this is an uncommon situation, it can occur periodically. To guarantee the continuous validity of the FileVault Personal Recovery Key (PRK) on the Jamf Pro server, we recommend creating an extra policy that executes a weekly command on an ongoing basis.

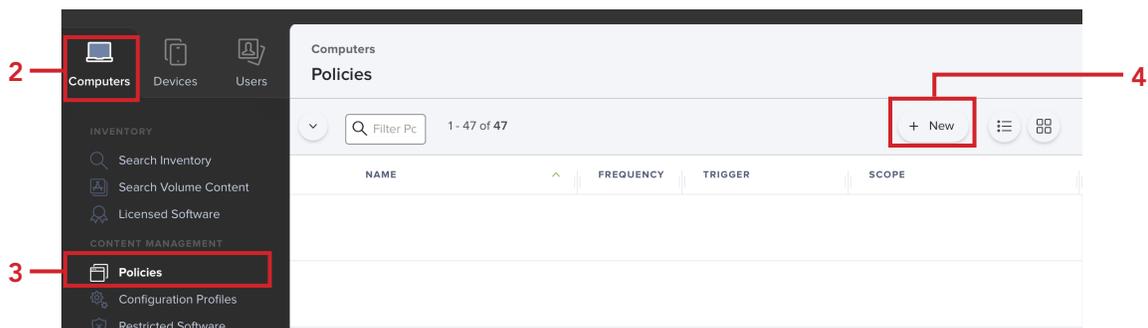
In this section, we will create a policy that runs the command below to re generate a FileVault Personal Recovery Key (PRK) at next login:

```
defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true
```

1. Log into your Jamf Pro Server.



2. Click Computers.
3. Click Policies.
4. Click New.





5. Configure the following:
  - A. Display Name: **Validate FileVault Key Escrow**
  - B. Category: **Security**
  - C. Trigger: **Recurring Check-in**
  - D. Execution Frequency: **Once every week**

General

**Display Name** Display name for the policy  
Validate FileVault Key Escrow **A**

Enabled

**Site** Site to add the policy to  
None

**Category** Category to add the policy to  
Security **B**

**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 event 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** **C**  
At the recurring check-in frequency configured in Jamf Pro

**Custom**  
At a custom event

**Execution Frequency** Frequency at which to run the policy  
Once every week **D**

6. Click on the Maintenance payload.
7. Click Configure.

The screenshot shows the Jamf Pro interface. On the left is a sidebar with a list of categories: Local Accounts (0 Accounts), Management Accounts (Not Configured), Directory Bindings (0 Bindings), EFI Password (Not Configured), Restart Options (Not Configured), and Maintenance (Not Configured). A red box labeled '6' highlights the 'Maintenance' item. The main content area shows the 'Configure Maintenance' screen with the text: 'Use this section to update inventory, reset computer names, install all cached packages, and run common maintenance tasks.' A red box labeled '7' highlights the 'Configure' button.



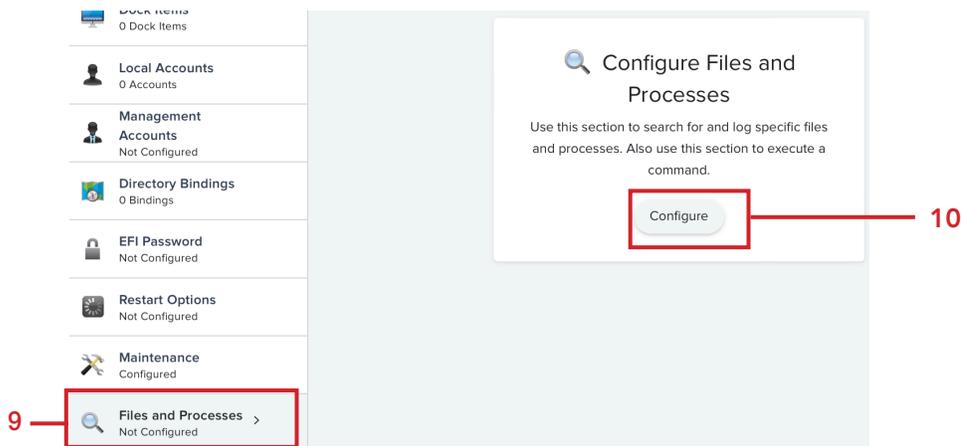
8. Confirm Update Inventory is enabled.

#### Maintenance

- Update Inventory**  
Force computers to submit updated inventory information to Jamf Pro
- Reset Computer Names**  
Change the computer name on computers to match the computer name in Jamf Pro
- Install Cached Packages**  
Install packages cached by Jamf Pro

9. Click on the Files and Processes payload.

10. Click Configure.



11. Enter the following command in the Execute Command field:

**defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true**

Files and Processes ✕

**Search For File By Path** Full path to the file

Delete file if found

**Search For File By Filename** Name of the file, including the file extension. This field is case-sensitive and returns partial matches

Update "locate" database  
Update the "locate" database before searching for the file

**Search For File Using Spotlight** File to search for. This field is not case-sensitive and returns partial matches

**Search For Process** Name of the process. This field is case-sensitive and returns partial matches

Kill process if found  
This works with exact matches only

**Execute Command** Command to execute on computers. This command is executed as the "root" user



12. Click Scope.
13. Click Targets.
14. Confirm Specific Computers is selected for Target Computers.
15. Click Add

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
--------	------

16. Click Computer Groups.
17. In the search field, enter **filevault**.
18. Click Add for "FileVault Encryption Key is Invalid or Unknown."
19. Click Save.

Options **Scope** Self Service User Interaction

Targets Limitations Exclusions

Add Deployment Targets Done

Computers **Computer Groups** Users User Groups Buildings Departments

filevault 1 - 1 of 1

GROUP NAME
FileVault Encryption Key is Invalid or Unknown

**Add**

Cancel **Save**

This policy will run once a week on all computers that show up in the smart computer group named FileVault Encryption Key is Invalid or Unknown. The FileVault key will be escrowed and the inventory in Jamf Pro to reflect the change.

This completes the guide.