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

Rev. 20230720

Contents

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

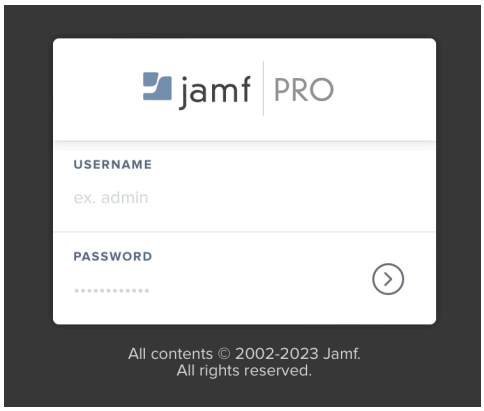
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software

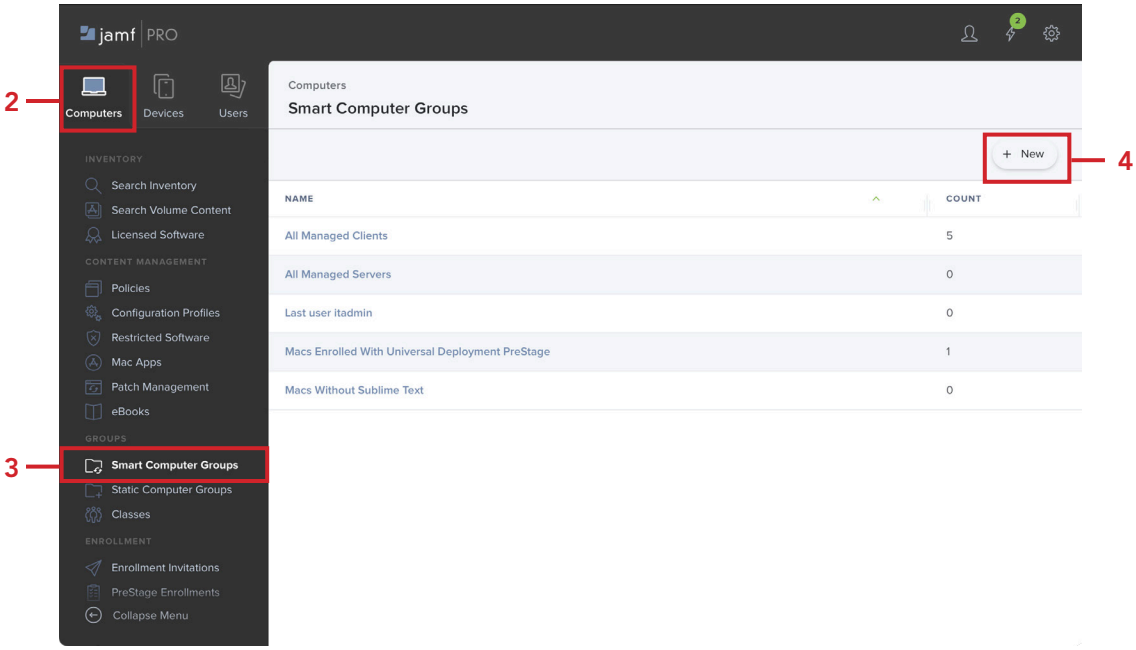
Requirements for following along with this section:

- 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

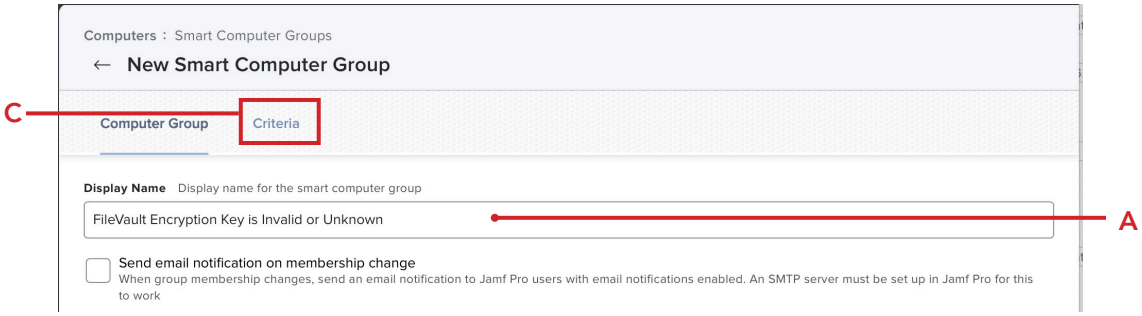
1. Log into your Jamf Pro server with administrative credentials.



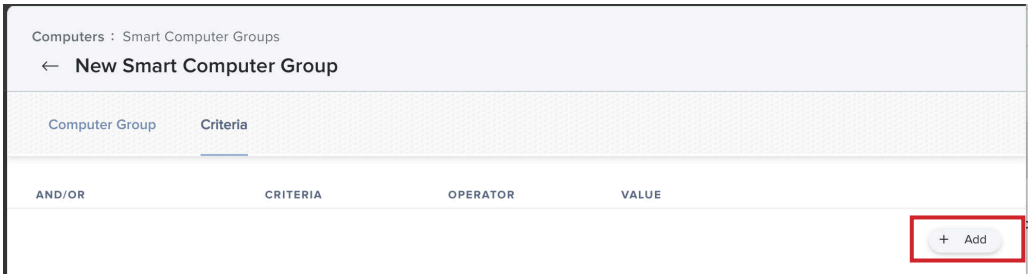
2. Click Computers
3. Click Smart Computer Groups.
4. Click New.



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

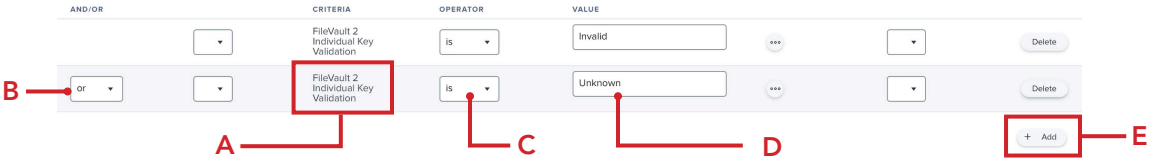


6. Click Add.

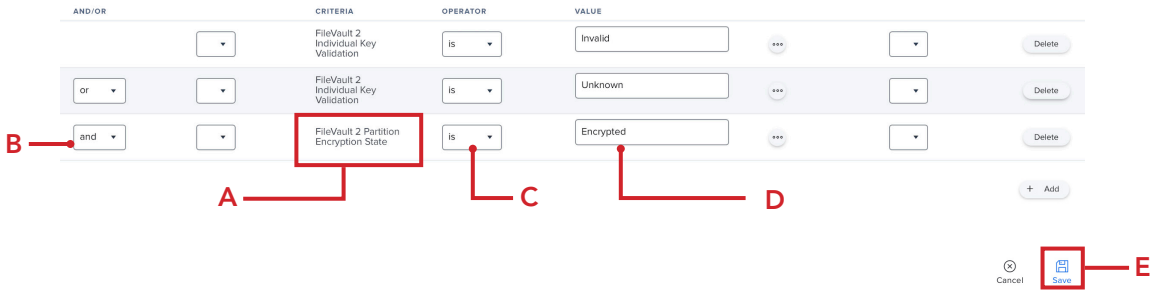


7. Configure the following for the Criteria as shown below:
   A. Criteria: **FileVault 2 Individual Key Validation**
   B. Operator: **is**
   C. Value: **Invalid**
   D. Click Add

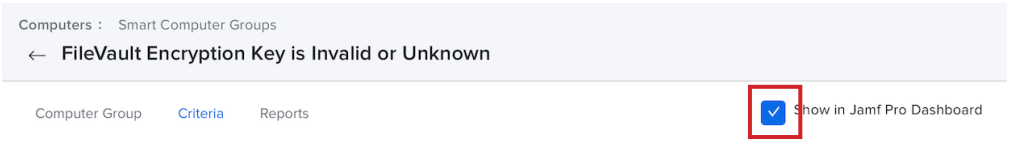
8. Configure the following for the Criteria as shown below:
   A. Criteria: **FileVault 2 Individual Key Validation**
   B. And/Or: **or**
   C. Operator: **is**
   D. Value: **Unknown**
   E. Click Add



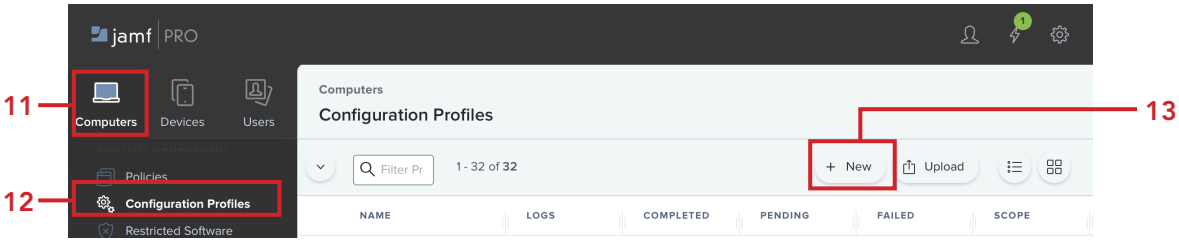
9. Configure the following for the Criteria as shown below:
   A. Criteria: **FileVault 2 Partition Encryption State**
   B. And/Or: **and**
   C. Operator: **is**
   D. Value: **Encrypted**
   E. Click Save



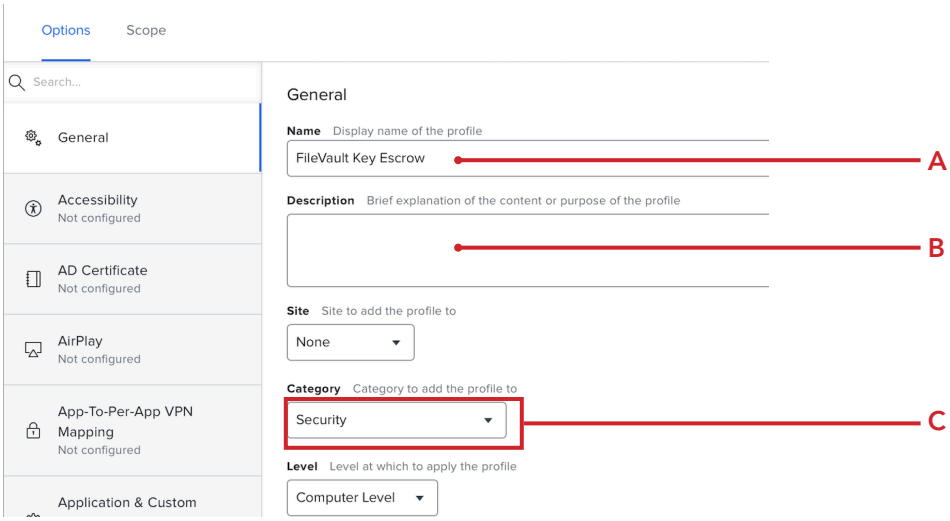
10. Select the checkbox for Show in Jamf Pro Dashboard.
    NOTE: We created this smart group to use for scoping later on in this guide.



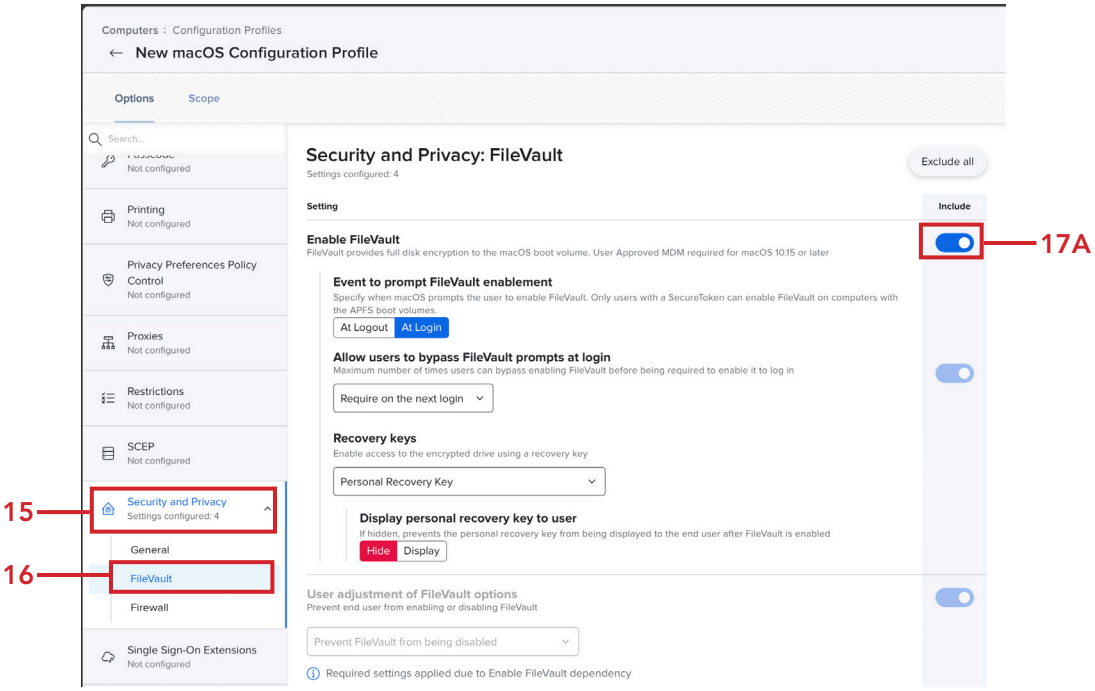
11. Click Computers.
12. Click Configuration Profiles.
13. Click New.



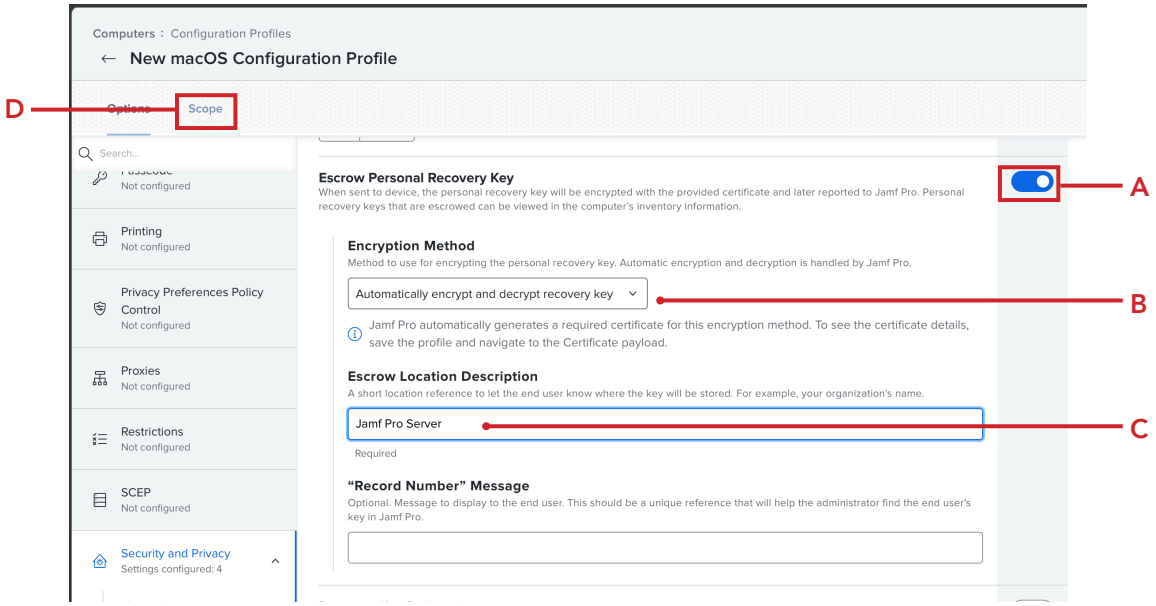
14. Click the General payload and enter the following:
    A. Name: **FileVault Key Escrow**
    B. Description: Add a description of your choosing if needed.
    C. Category: This guide will use Security. Feel free to select a category of your choosing.
    D. Leave all other items at their default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



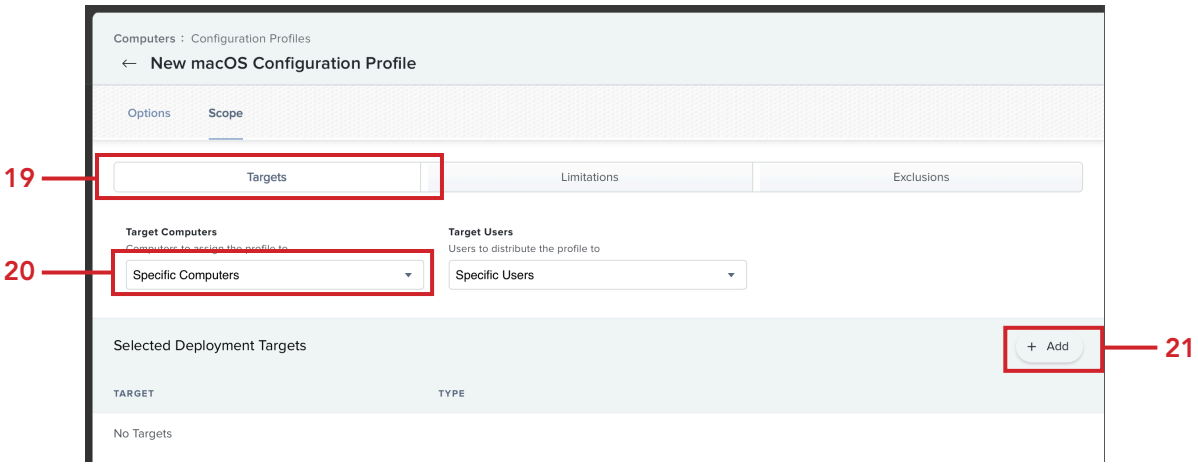
15. Scroll down and click Security and Privacy payload
16. Click FileVault.
17. Configure the following:
    A. Enable FileVault: **Enable**
    B. Scroll down to Escrow Personal Recovery Key.



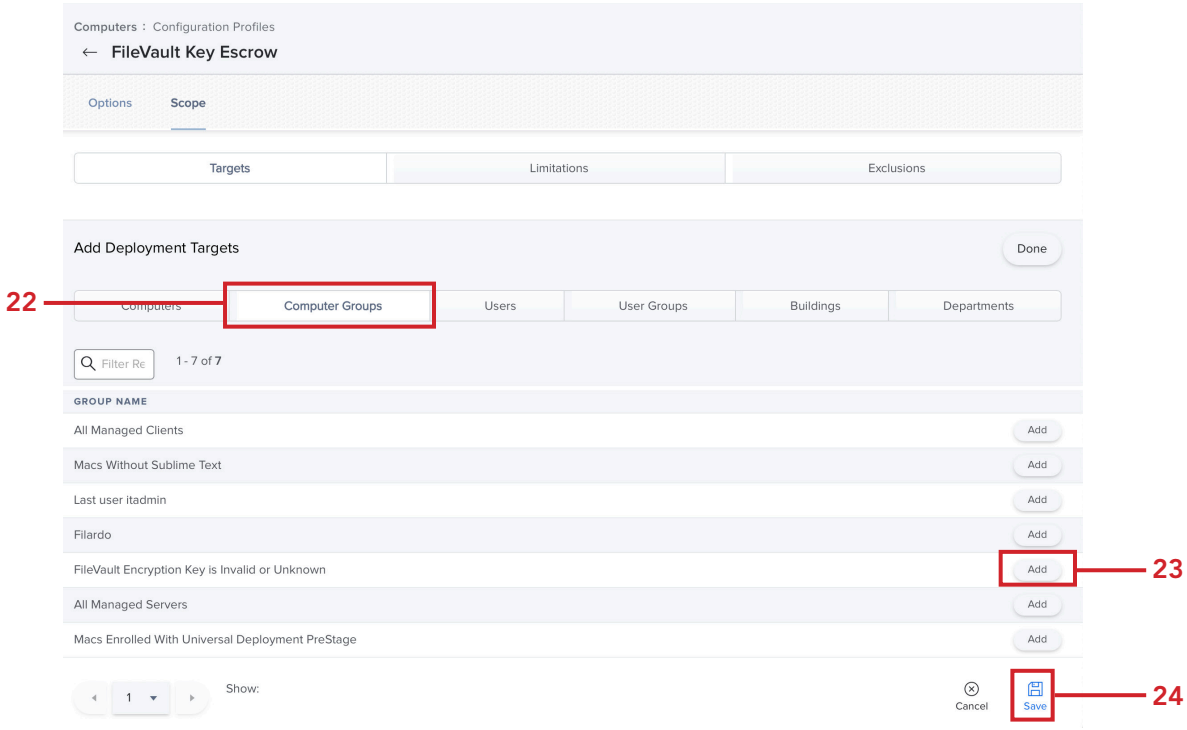
18. Configure the following:
    A. Escrow Personal Recovery Key: **Enable**
    B. Encryption Method: **Automatically encrypt and decrypt recovery key**.
    C. Escrow Location: **Jamf Pro Server**.
    D. Click Scope.



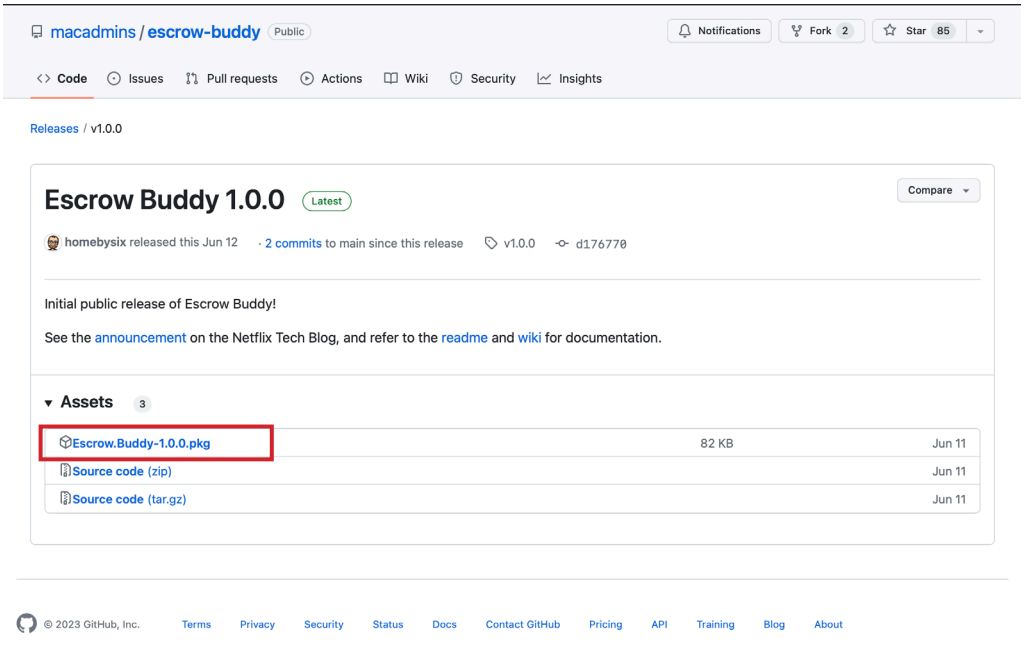
19. Click Targets
20. Confirm Specific Computers is selected for Target Computers.
21. Click Add



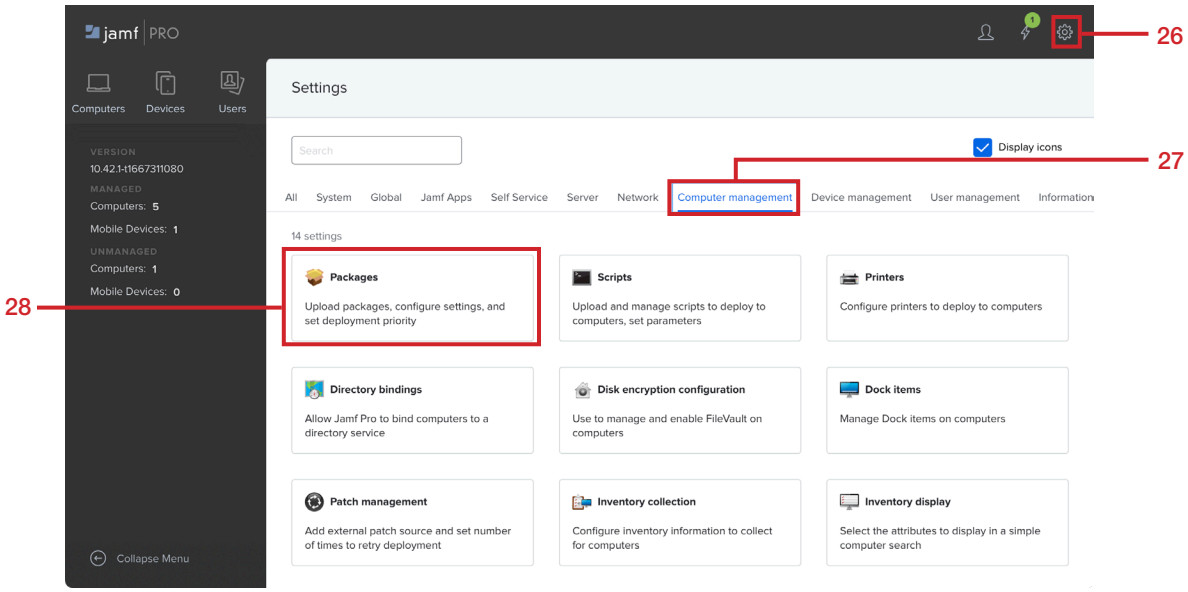
22. Click Computer Groups.
23. Click Add for "**FileVault Encryption Key is Invalid or Unknown.**"
24. Click Save.



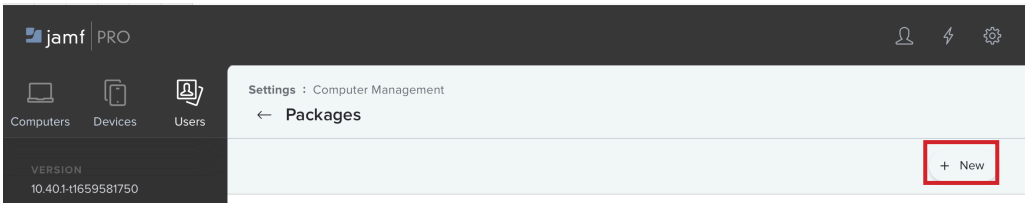
25. Download Escrow Buddy.
    https://github.com/macadmins/escrow-buddy/releases/latest



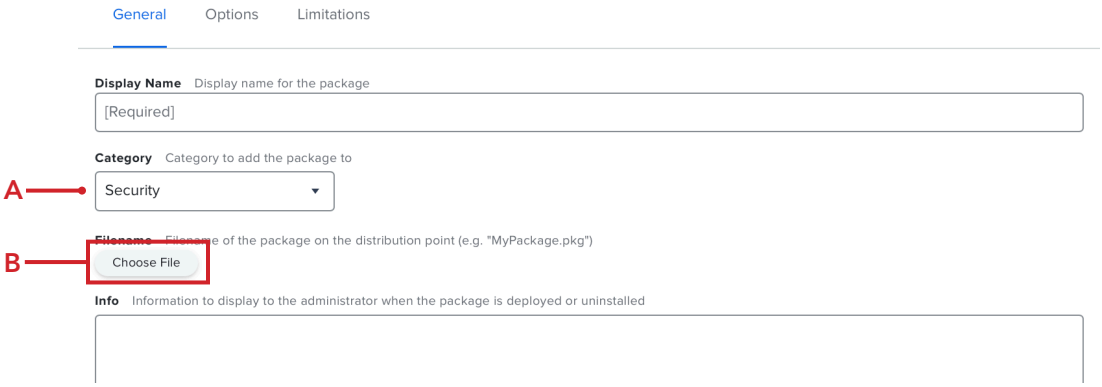
26. Switch back to your Jamf Pro Server instance. On the top-right corner, click Settings (⚙).
27. Click Computer management.
28. Click Packages.



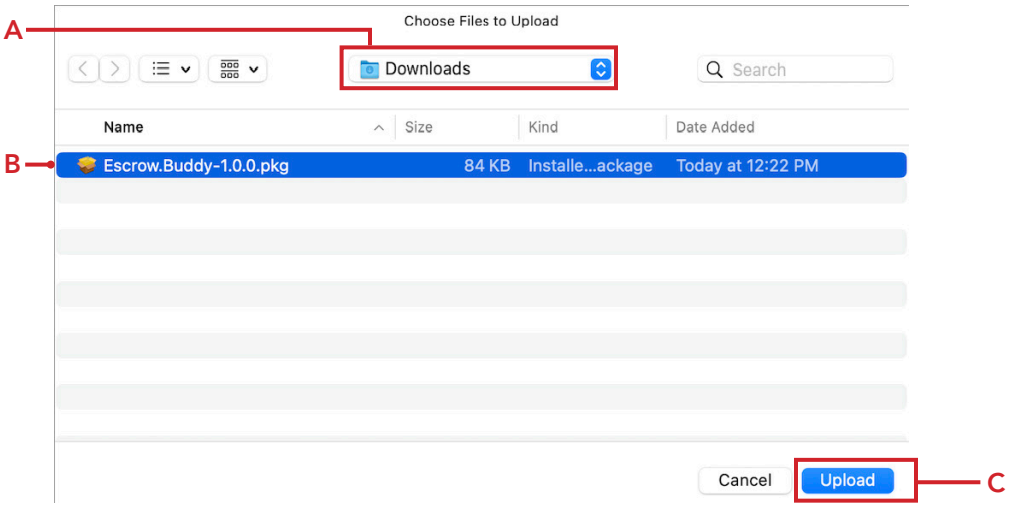
29. Click New.



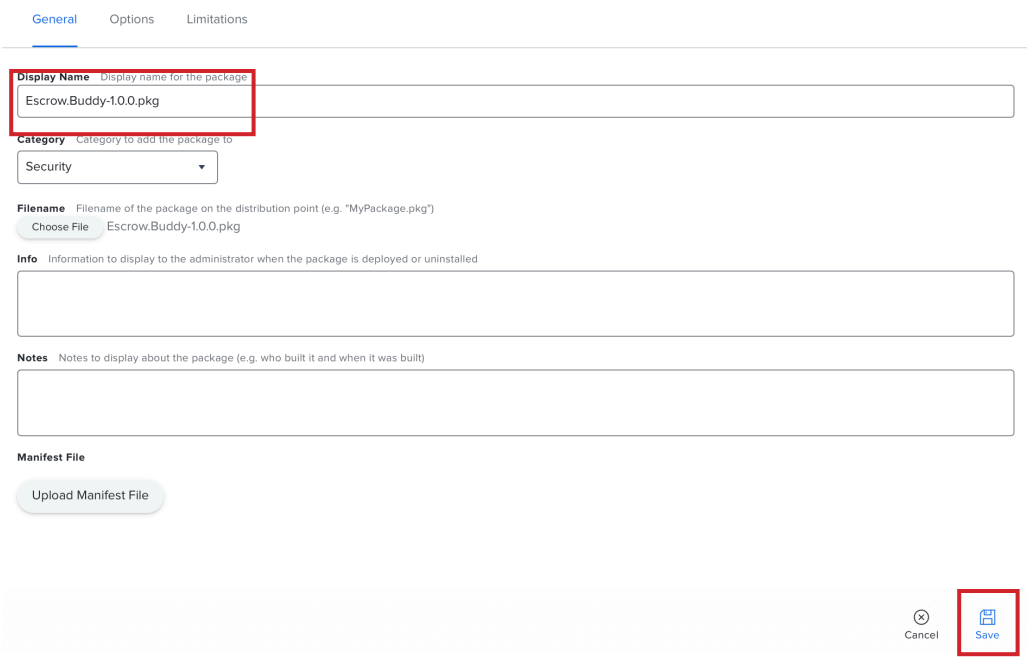
30. Configure the following:
    A. Category: This guide will use Security
    B. Click Choose File



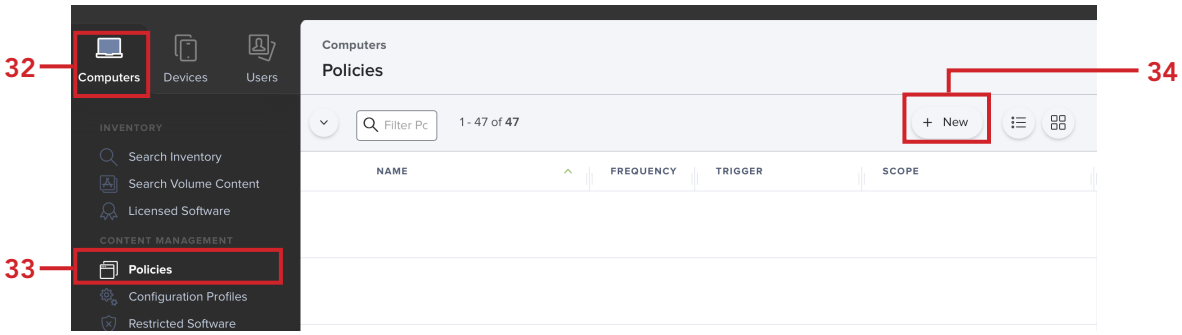
30. Perform the following:
    A. Navigate to your Downloads folder
    B. Select Escrow.Buddy-1.0.0.pkg
    C. Click Upload



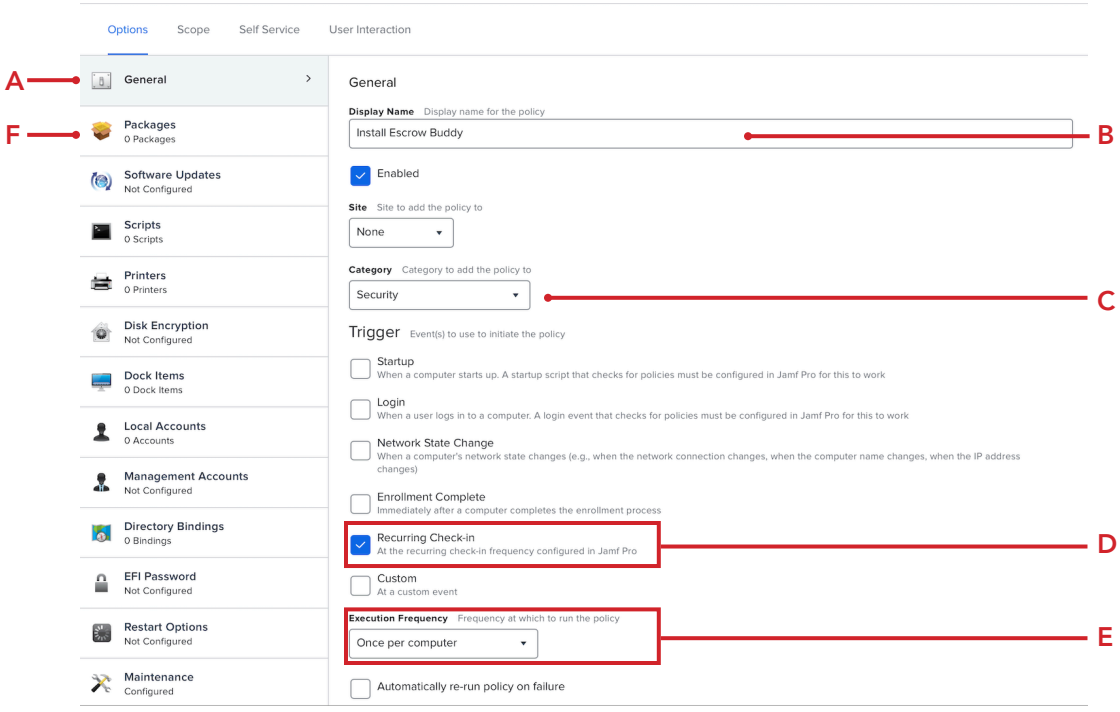
31. Confirm the Display Name auto-populates with the name Escrow.Buddy-1.0.0.pkg. Click Save.



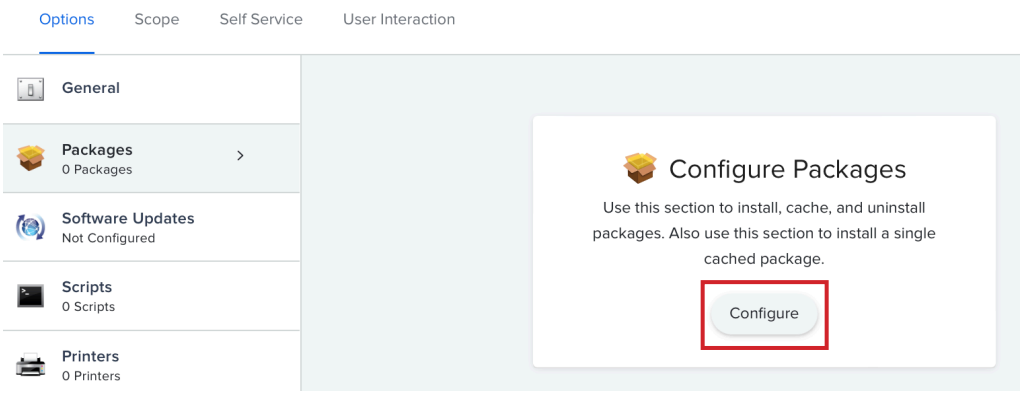
32. Click Computers.
33. Click Policies.
34. Click New.



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

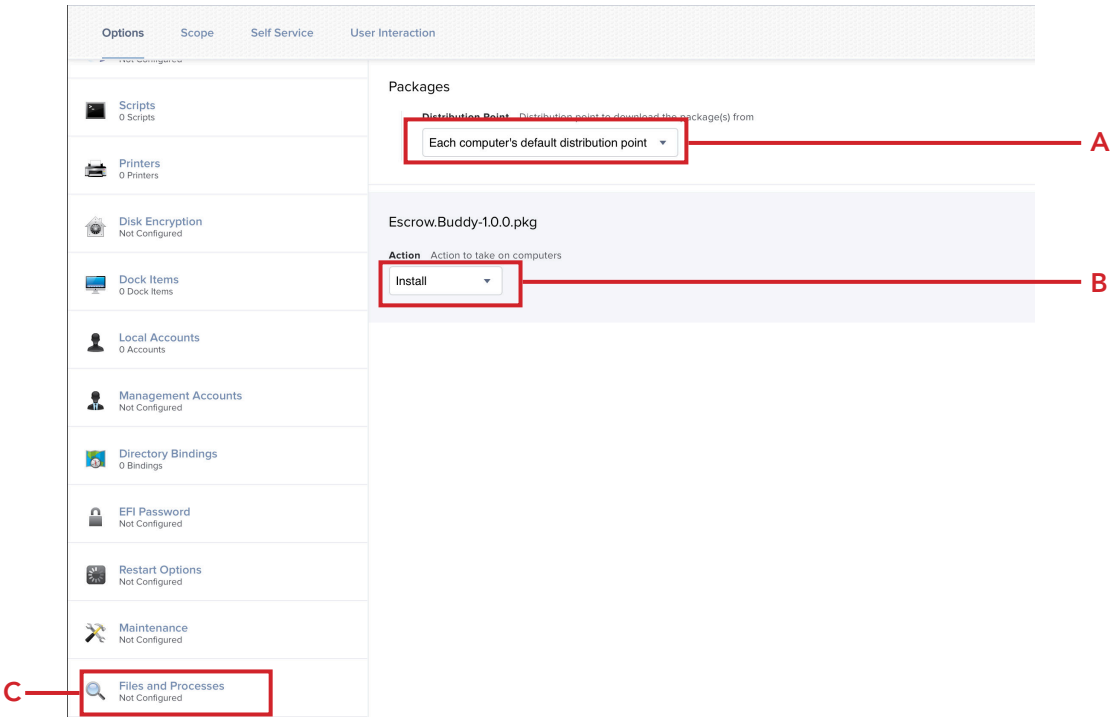


36. Click Configure.

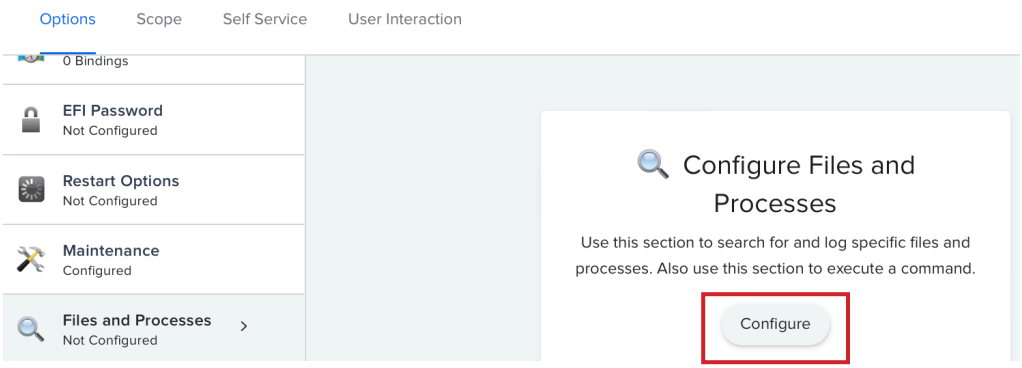


37. Click Add for Escrow.Buddy-1.0.0.pkg.

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.

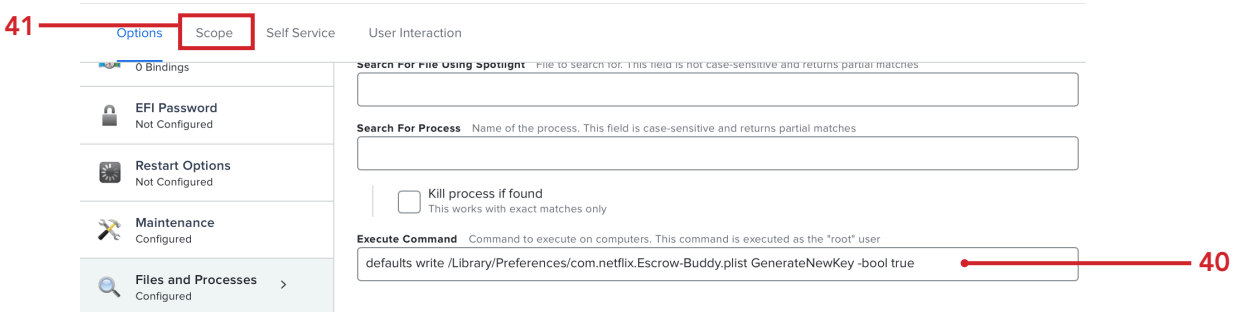


40. In the Execute Command field, enter the following:

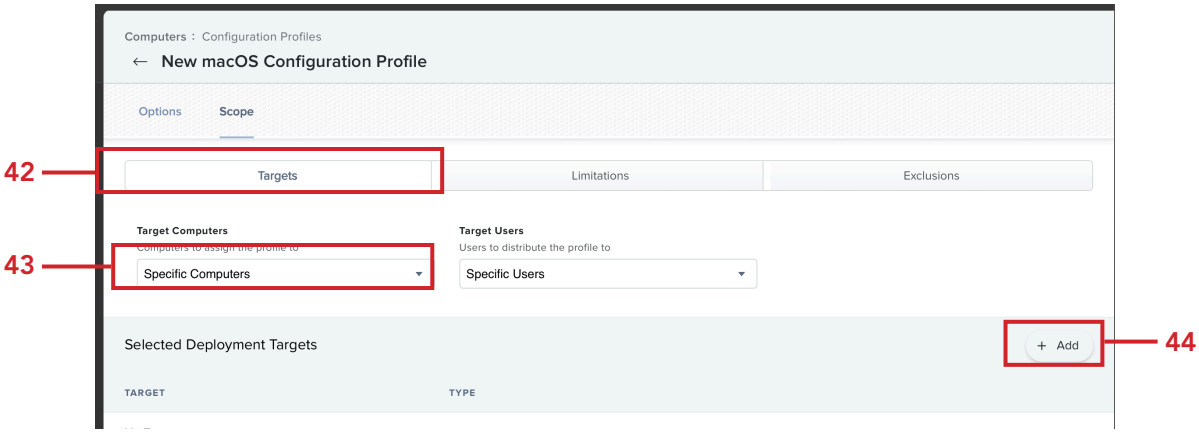
```
defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true
```

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

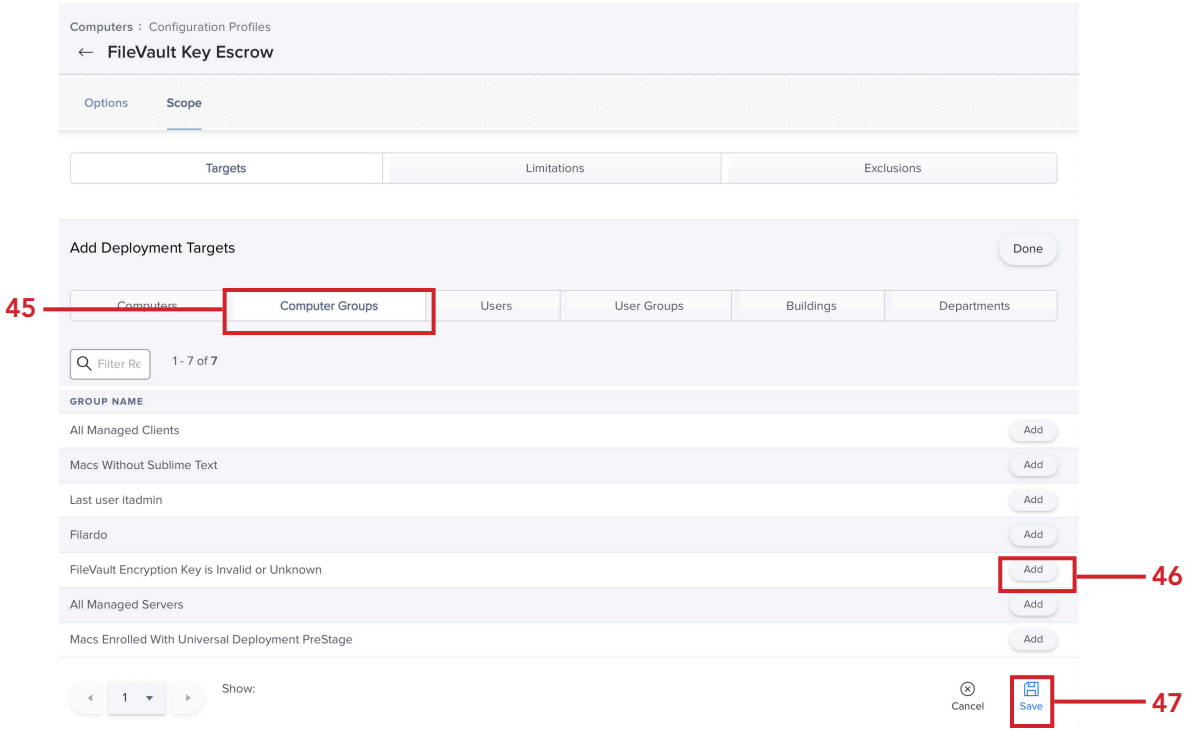
41. Click Scope.



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.



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

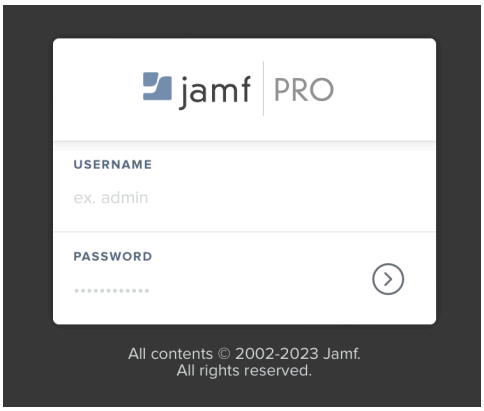
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software

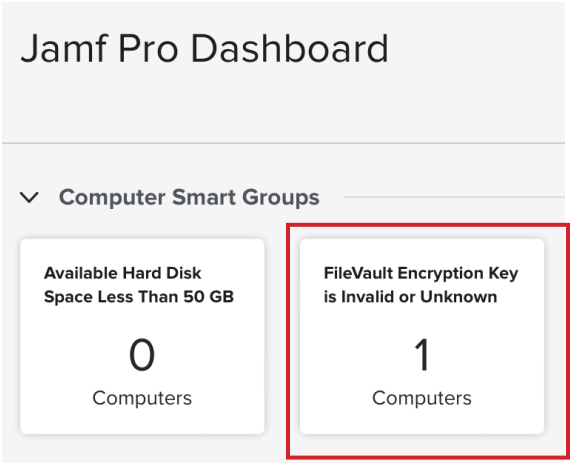
Requirements for following along with this section:

- A Mac with macOS Mojave 10.14.4 or later with FileVault enabled and NOT enrolled in Jamf Pro.
- Jamf Pro administrator credentials

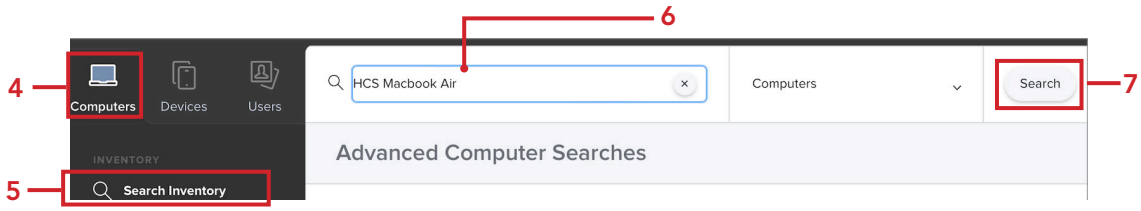
1. Enroll your Mac computer into the Jamf Pro server. This can be done via User Initiated Enrollment or an Enrollment Invitation email if SMTP is configured on your Jamf Pro server.
2. Log into your Jamf Pro Server.



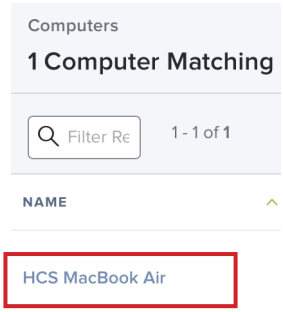
3. The Jamf Pro Dashboard should show at least one computer in the "FileVault Encryption Key is Invalid or Unknown" Smart Computer Group.



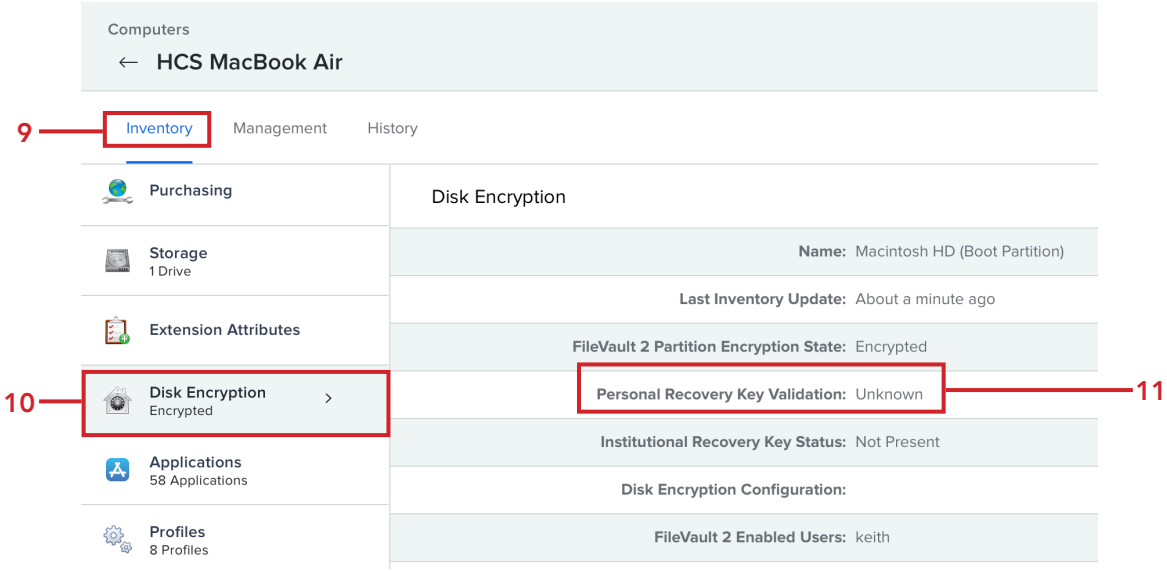
4. Click Computers.
5. Click Search Inventory
6. In the search field, enter the name of the computer you just enrolled
7. Click Search



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 — 149×34
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-jcds.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 ~ %
```

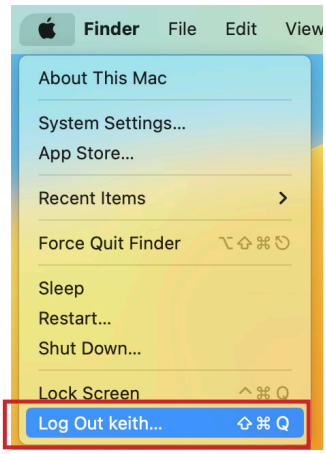
14. Enter the command below to ensure the inventory is updated on the Jamf Pro server.

```
sudo jamf recon
```

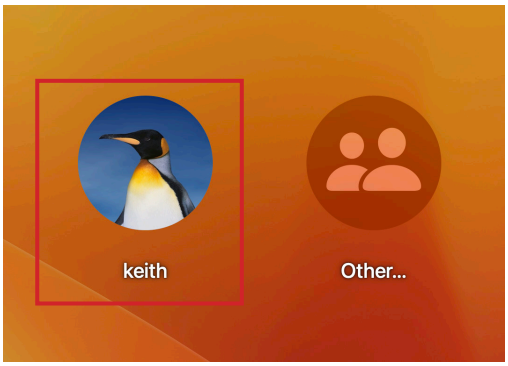
Enter your administrator password if required.

```
keith — -zsh — 90×29
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 ~ %
```

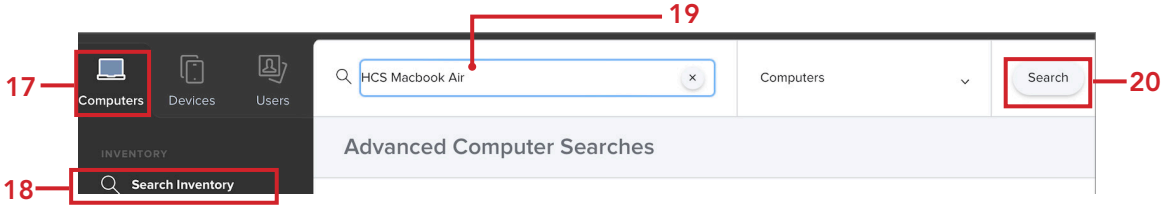
15. Log out of your Mac computer.



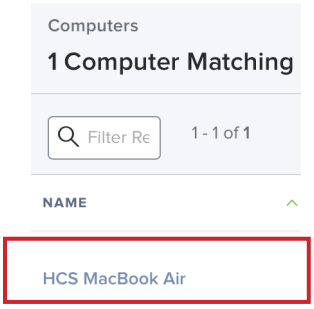
16. Log back into your Mac computer. Escrow Buddy will initiate the FileVault Re-Key and escrow the key in the Jamf Pro server.



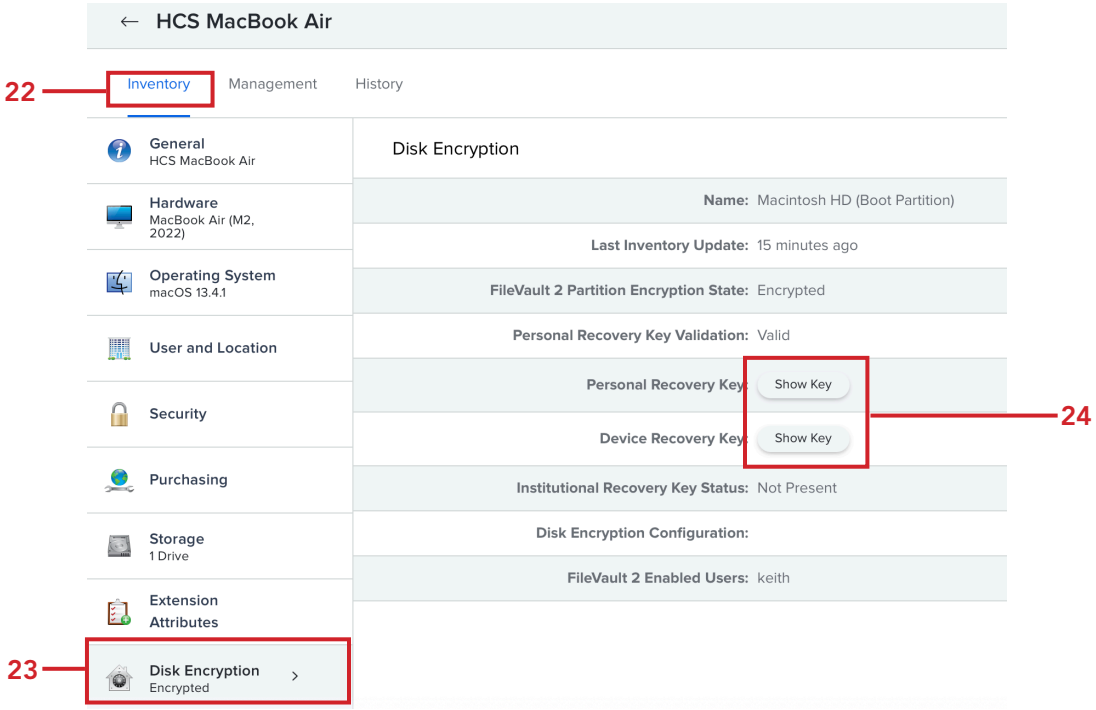
17. Switch back to your Jamf Pro server. Click Computers
18. Click Search Inventory
19. In the search field, enter the name of the computer you just enrolled
20. Click Search



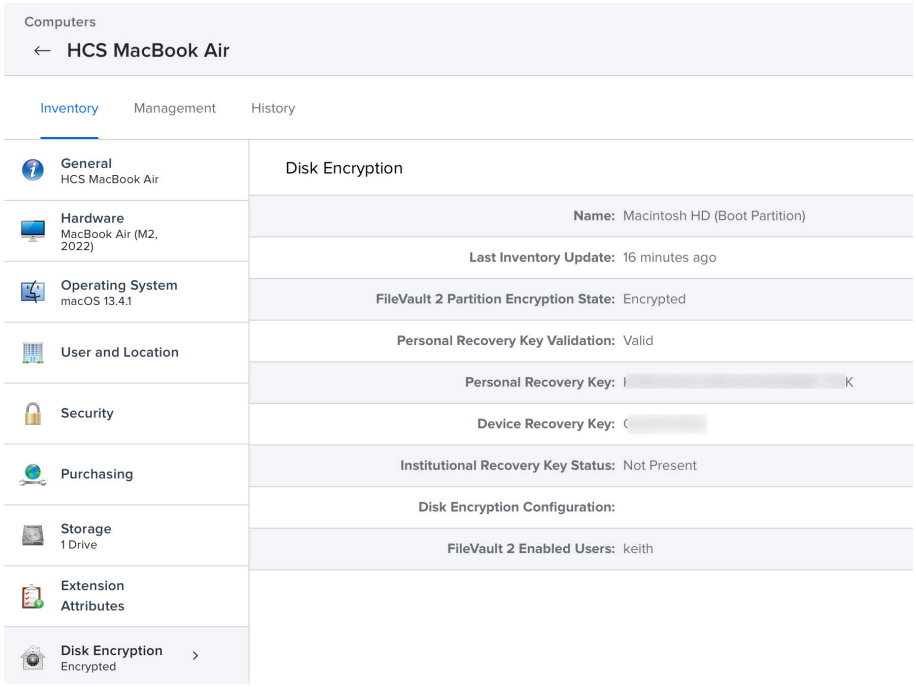
21. Select your Mac computer.



22. Click Inventory.
23. Click Disk Encryption.
24. Verify the Personal Recovery Key and the Device Recovery Key both have Show Key buttons.



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



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:

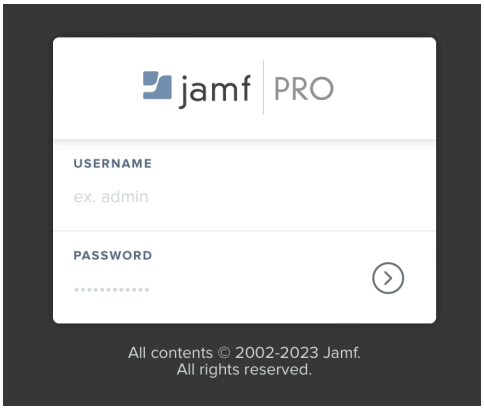
- Jamf Pro administrator credentials

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.

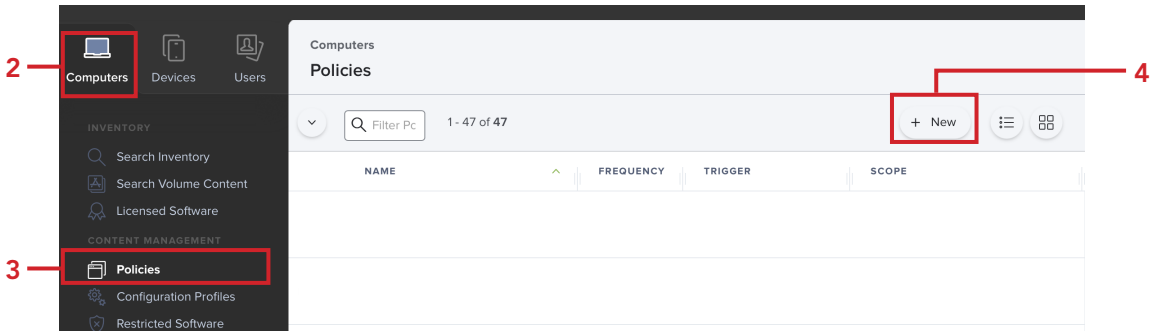
In this section, we will create a policy that runs the command below to re generate a FileVault Personal Recovery Key (PRK) at next login:

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

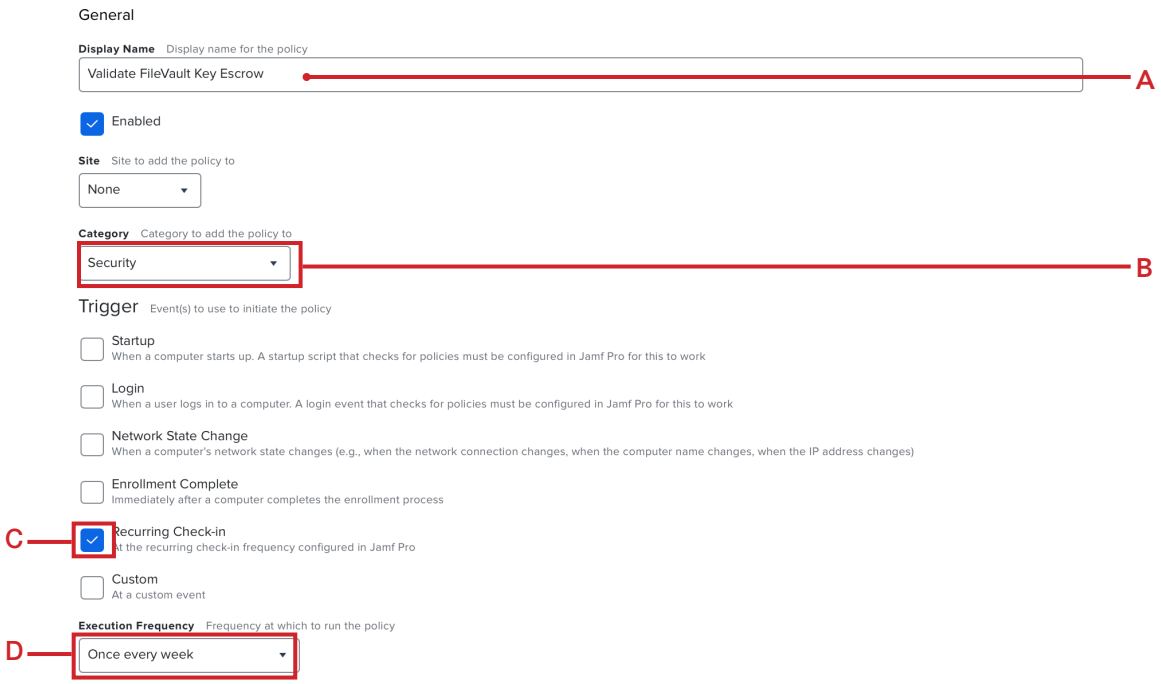
1. Log into your Jamf Pro Server.



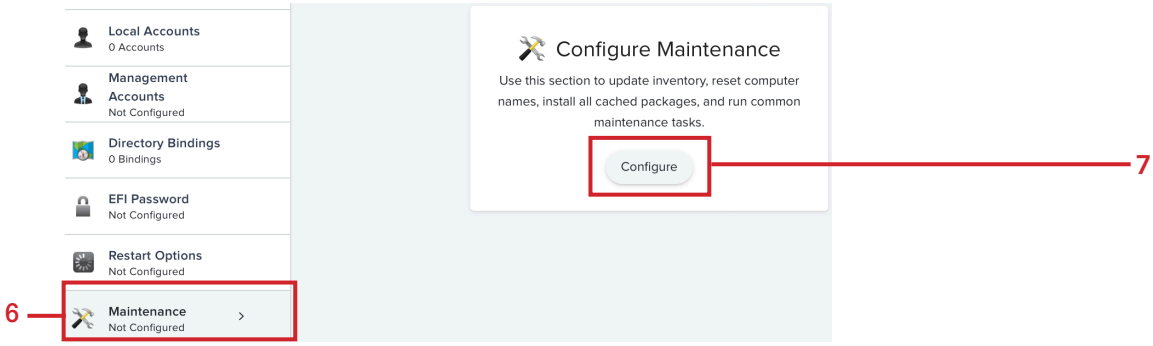
2. Click Computers.
3. Click Policies.
4. Click New.



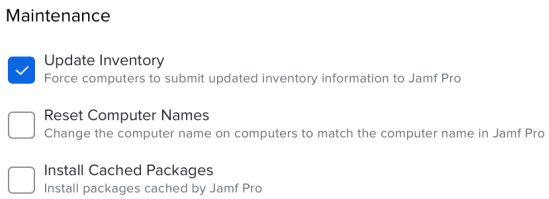
5. Configure the following:
   A. Display Name: **Validate FileVault Key Escrow**
   B. Category: **Security**
   C. Trigger: **Recurring Check-in**
   D. Execution Frequency: **Once every week**



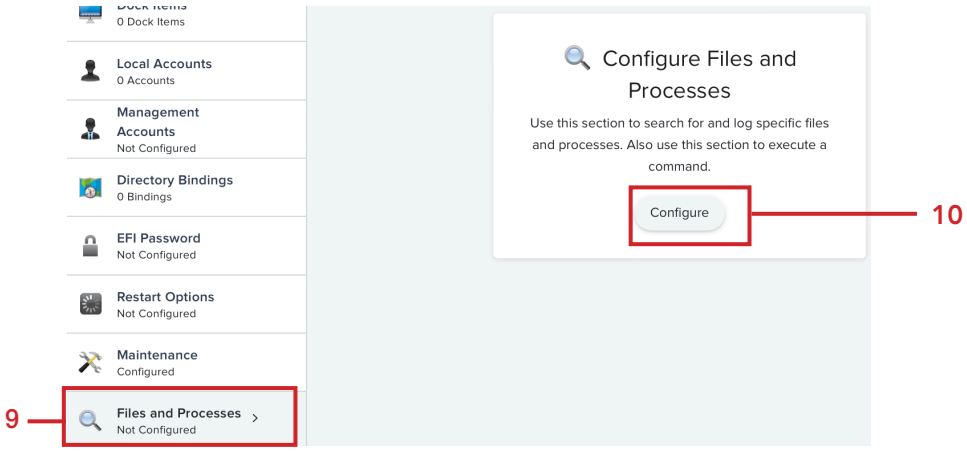
6. Click on the Maintenance payload.
7. Click Configure.



8. Confirm Update Inventory is enabled.

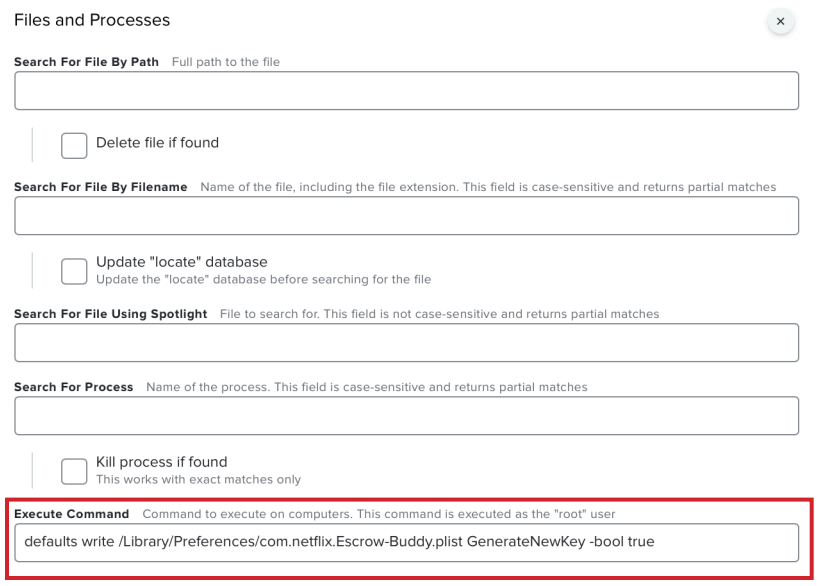


9. Click on the Files and Processes payload.
10. Click Configure.

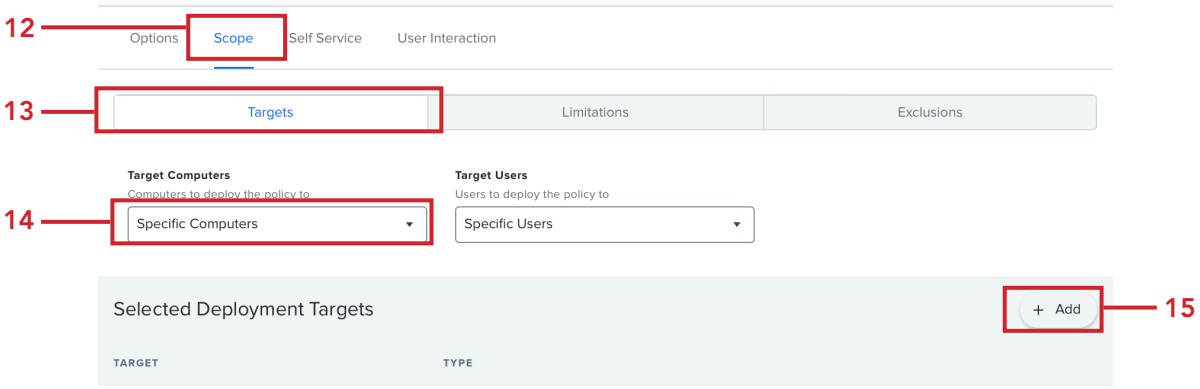


11. Enter the following command in the Execute Command field:

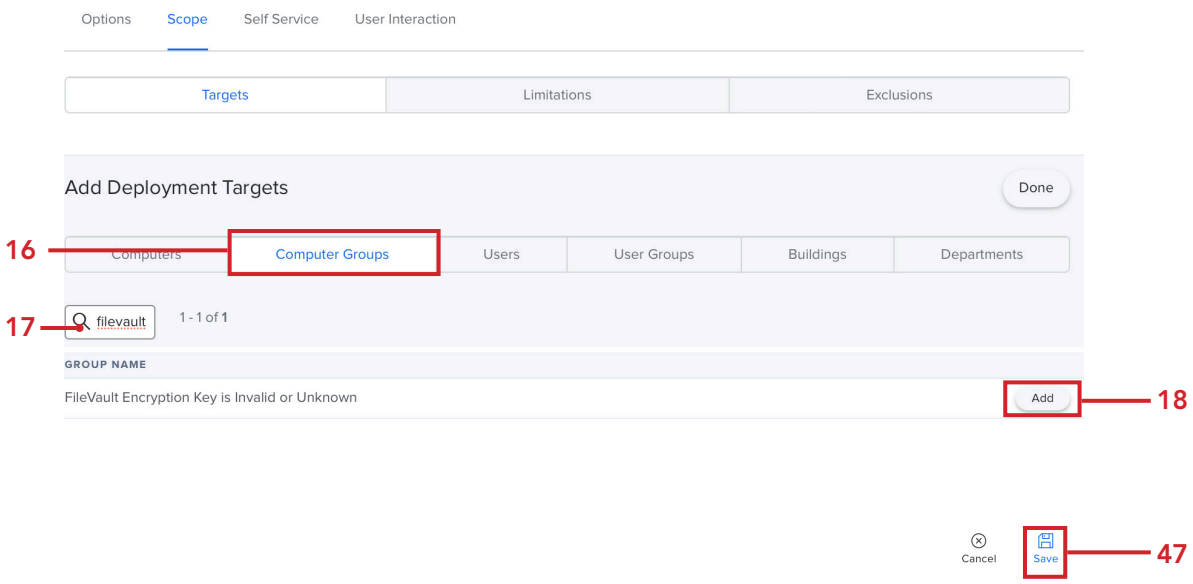
```
defaults write /Library/Preferences/com.netflix.Escrow-Buddy.plist GenerateNewKey -bool true
```



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



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.



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.