jamf | PRO

How to Deploy and Configure
Jamf Setup Manager

Contents

Preface

What is Jamf Setup Manager?
Jamf Setup Manager builds upon the robust feature sets of Baseline and DEP Notify utilities, providing a pivotal solution for IT departments and provisioning depots. Its primary purpose is to ensure that new Macs are configured and assigned before they are distributed to the end-users. Setup Manager runs seamlessly over Setup Assistant, preceding user creation, thereby avoiding any interference with MDM-capable users or the secure token flow for FileVault. This process is as elegant as it is secure. Through the use of a configuration profile, you can control which policies and installations Setup Manager executes, giving you complete oversight and flexibility.

*The Jamf Setup Manager Package also comes pre-loaded with Installomator and SwiftDialog.

FileVault and Software Versioning Setup
In this guide, we will configure FileVault for automatic enablement through Automated Device Enrollment (ADE) and setup the minimum required macOS version payload.

Requirements
The minimum requirements for your Apple devices:
- A Jamf Pro Server running version 11.9 or later
- A Jamf Pro account with Administrator Privileges
- A Mac computer running macOS 14.5 or later

Jamf Setup Manager Github:
https://github.com/Jamf-Concepts/Setup-Manager

Jamf Concepts to download setup manager:
https://concepts.jamf.com

HCS Show Me Your ID 3.0:
https://hcsonline.com/support/apps/show-me-your-id

Jamf Setup Manager: Workflow and Execution
How does Jamf Setup Manager Work?

1. Configuration Profile Setup: Jamf Setup Manager is configured using a configuration profile. This profile defines how the setup assistant will install apps, deploy packages, and apply branding. We will use a PreStage enrollment to install the Jamf Setup Manager package during Automated Device Enrollment.

2. Enrollment Actions: Within the configuration profile, the Enrollment Actions section lists the specific tasks to be performed during the setup process. These actions can include installing packages by triggering Jamf policies.
NOTE: This guide will focus on installing packages from Jamf Pro using a custom policy trigger.

3. Package Installation using Policies:
    • Packages are deployed using custom policy trigger set in the configuration profile.
    • Packages are installed using Installomater which is built into Jamf Setup Manager

4. Branding Application:
    • Custom branding is applied by specifying an Icon Source, Title, and Message in the configuration profile.
    • These branding elements are displayed during the setup process, providing a personalized experience for the user.

5. Setting custom attributes when Jamf Setup Manager is running:
    • Setting a computer name
    • Setting an Asset tag

6. Final Action: Once all the specified tasks (app installs, package deployments, branding) are complete, Setup Manager concludes with a Final Action, such as restarting the system or completing the setup assistant.

7. Clean Up: Setup Manager creates a flag file at /private/var/db/.JamfSetupEnrollmentDone when it finishes. If this file exists when Setup Manager launches, the app will terminate immediately and without taking any action.

This guide covers:
Configuration of Jamf Setup Manager
        A. Creating a Category
        B. Creating a Smart Computer Group
        C. Creating a Configuration Profile for Jamf Setup Manager
        D. Creating a package with Jamf Composer
        E. Uploading packages to Jamf Pro
        F. Creating a policy to install packages
        G. Creating a PreStage Enrollment using Jamf Setup Manager

Section 1: Jamf Pro Preparation for Setup Manager

What you will need:
This section outlines the hardware, software, and necessary prerequisites to follow along with the Jamf Setup Manager guide.

Hardware and Software:
To complete the tasks outlined in this guide, ensure that you have the following hardware and software. Download the items from the links provided below:

- Jamf Setup Manager:
  https://github.com/Jamf-Concepts/Setup-Manager/releases
- HCS Show Me Your ID 3.0:
  https://hcsonline.com/support/apps/show-me-your-id
- HCS Logo:
  https://hcsonline.com/images/HCS_Logo.svg
- Jamf Composer:
  https://account.jamf.com/login
- Jamf Pro Server (Version 11.9):
  Ensure you are working with Jamf Pro server 11.9 or later to utilize the features and functionalities outlined in this guide.
- A Non-Production Mac with macOS 14.5:
  The Mac should be enrolled in Apple Business Manager (ABM) or Apple School Manager (ASM) and assigned to your Jamf Pro server.
- Required Downloads:
  This guide assumes that all downloaded files and software are stored in your Downloads folder for ease of access throughout the guide.

  Jamf Setup Manager Github:
  https://github.com/Jamf-Concepts/Setup-Manager

  Jamf Concepts to download setup manager:
  https://concepts.jamf.com

  HCS Show Me Your ID 3.0:
  https://hcsonline.com/support/apps/show-me-your-id

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

2. Click Settings.

3. Click Global.

4. Click Categories.

5. Click New.

6. Enter **Jamf Setup Manager** for the Display Name.

7. Click Save.
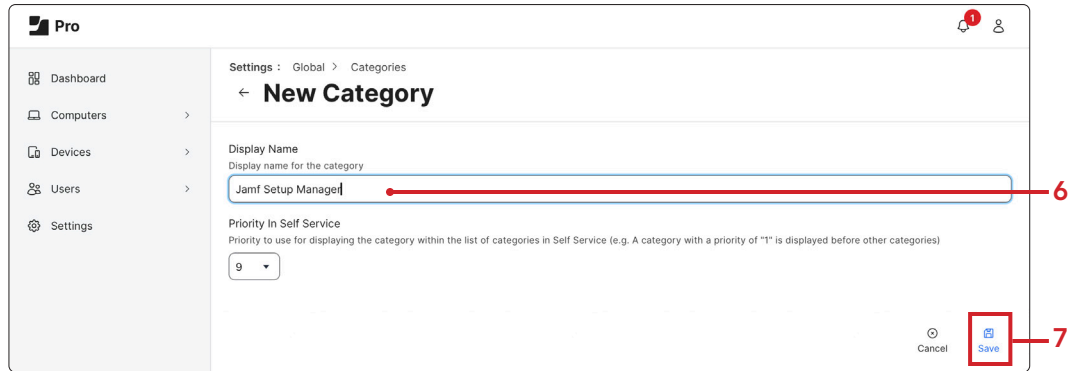
8. Click Computers.

9. Click PreStage Enrollments.

10. Click New.
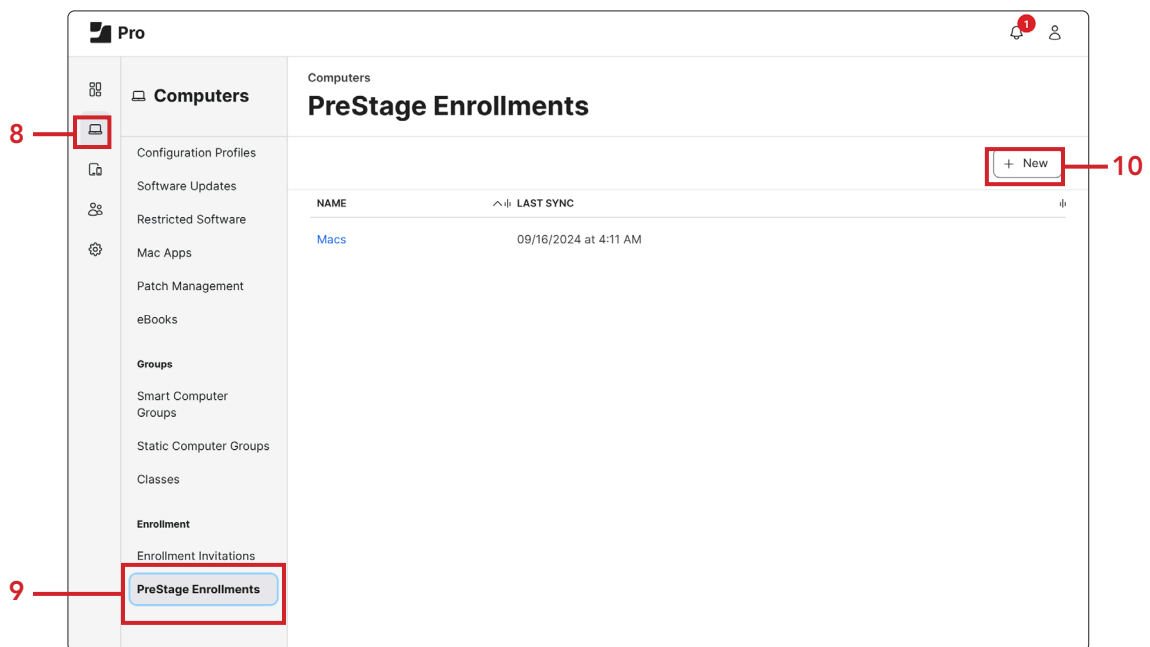
11. Enter **Jamf Setup Manager** for the Display Name.

12. Click Save. We will finish the configuration of the PreStage in Section 7 of this guide.
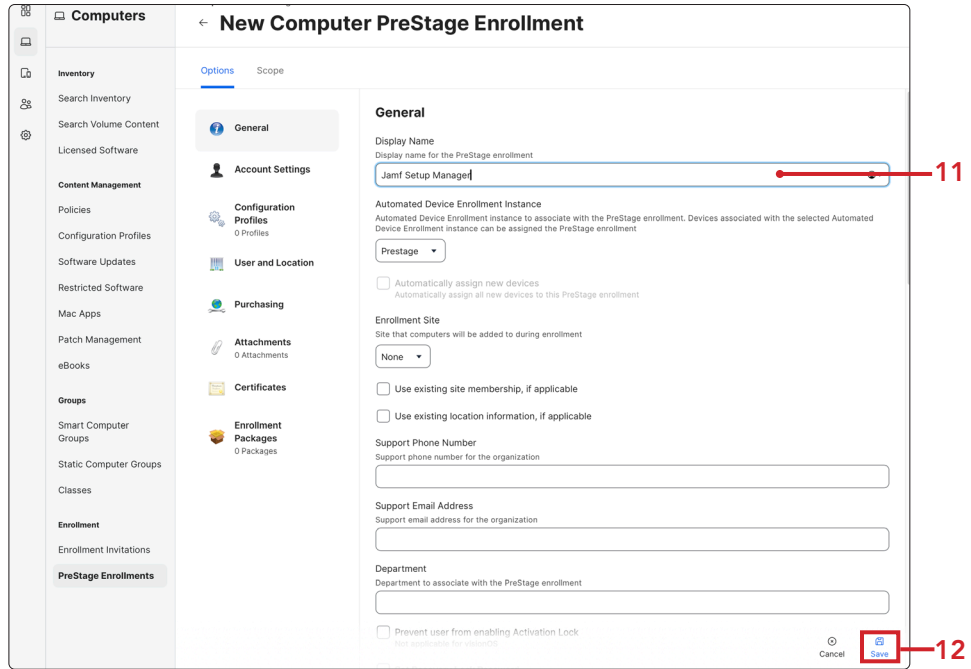
13. Click Computers.

14. Click Smart Computer Groups.

15. Click New.
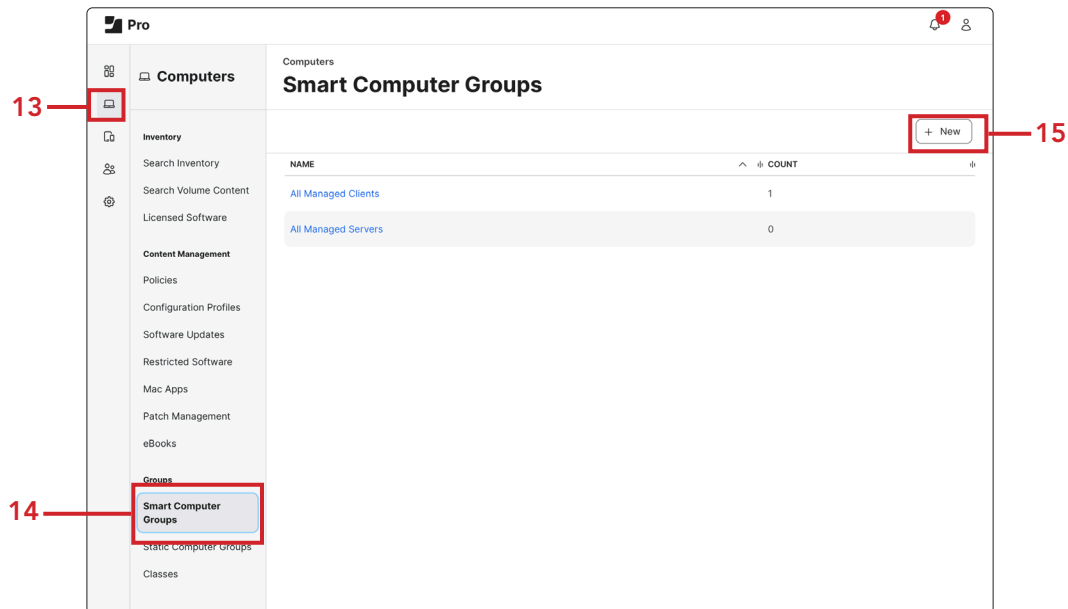
16. For the Display Name, enter **Macs Enrolled with Jamf Setup Manager PreStage**.

17. Click Criteria.

18. Click Add.

19. Click Show Advanced Criteria.

20. Scroll to Enrollment Method: PreStage Enrollment.

21. Click Choose.

22. Click Browse (···).

23. Choose Jamf Setup Manager.

24. Click Save.

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

Section 2: Create a Jamf Setup Manager Configuration Profile

Overview

In this section, we will configure and deploy the Jamf Setup Manager configuration profiles using Jamf Pro. Jamf Pro makes this process straightforward with a built-in template that simplifies the creation and deployment of configuration profiles to macOS devices. At the end of the section we will create a configuration profile that will be used in to enable FileVault at enrollment.

1. Click Computers.

2. Configuration Profiles.

3. Click New.
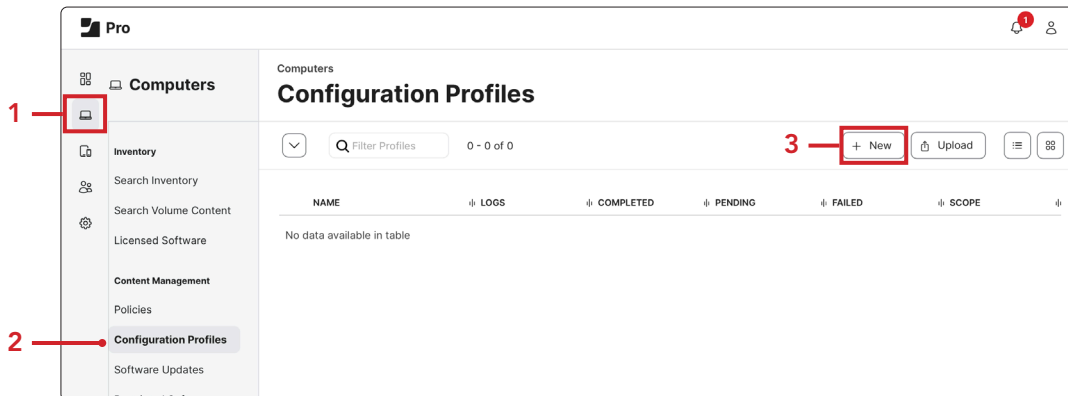
4. Enter **Jamf Setup Manager** for the name. The Jamf Setup Manager Profile defines how the setup assistant installs apps, deploys packages, applies custom branding and allows the manual creation of computer name and asset tags during Automated Device Enrollment (ADE).

5. Set the Category to Jamf Setup Manager.

6. Click on Application & Custom Settings.
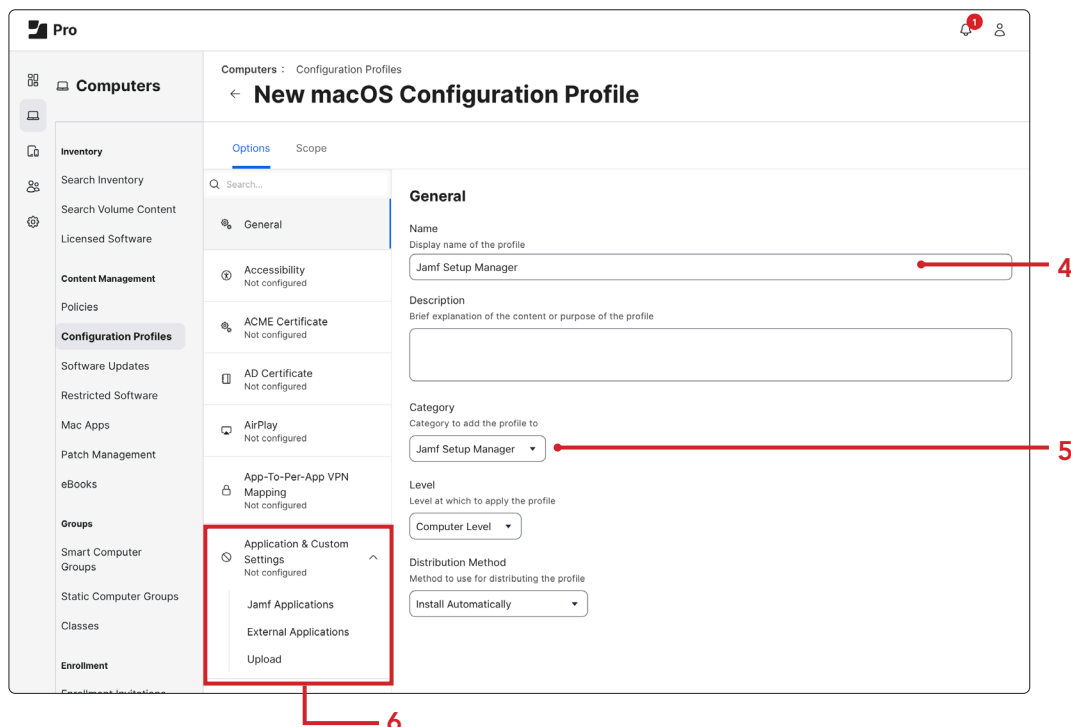
7. Click Jamf Applications.

8. Click Add.
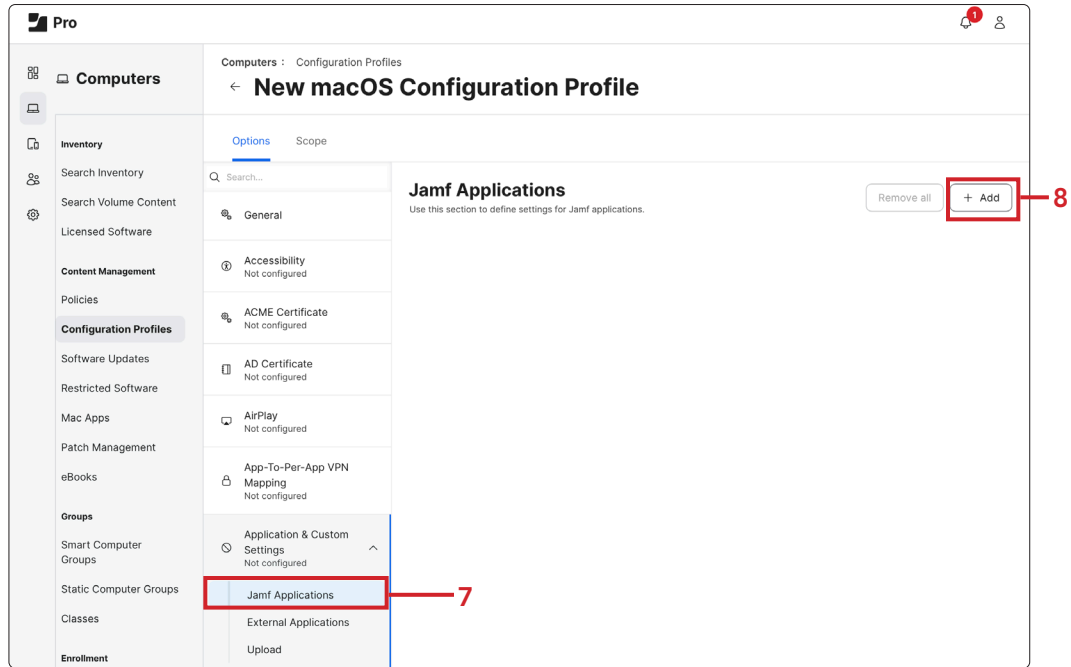
9. Click on the Jamf Application domain menu.

10. Select com.jamf.setupmanager.
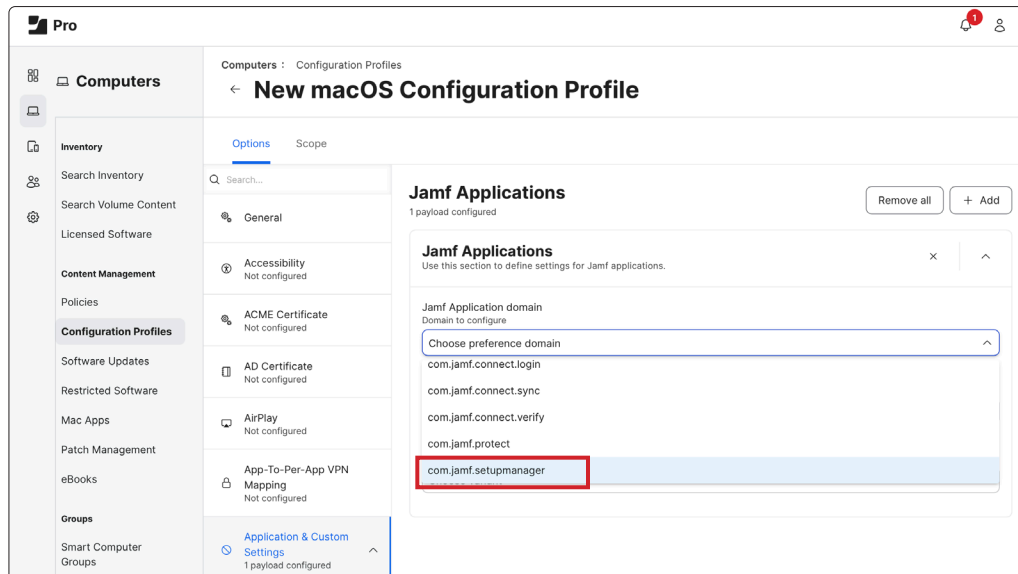
11. Select the following:
    A. Version:1.0
    B. Variant: Setup Manager.json
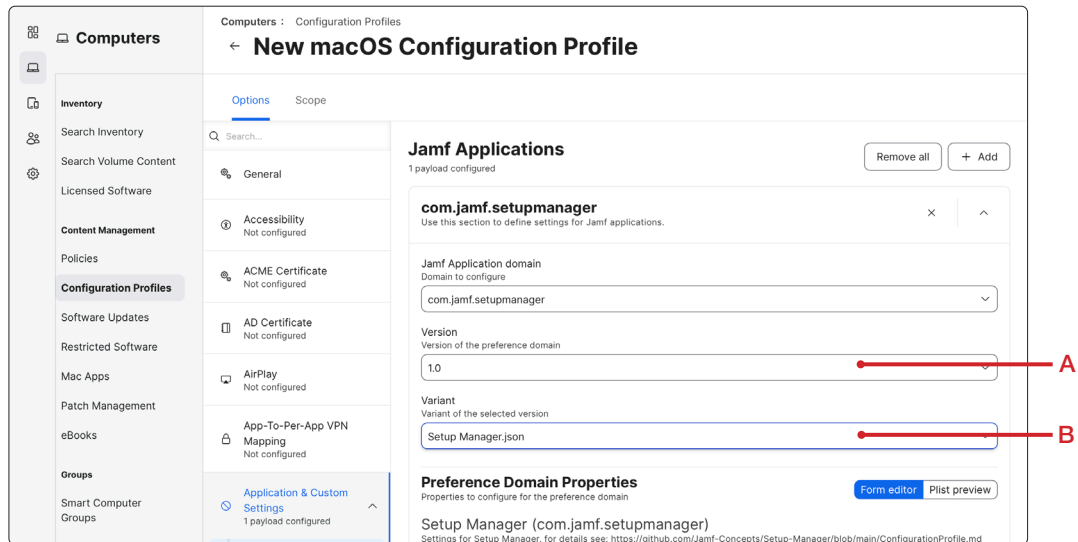
12. Let's configure the icon, title and message we would like for the employee to see when they enroll the Mac for the first time. Scroll down to Preference Domain Properties.
    A. Icon Source - This can come from a URL, path to an application where the icon will be pulled automatically if the application exists on the Mac or through SF Symbols which will not be discussed in this guide. This guide will use the link below.

    https://hcsonline.com/images/HCS_Logo/HCS_Logo_iOS.png

    B. Title - Add your organization here. This guide will use HCS Technology Group.
    C. Message - A message you want to display to your users. This guide will use Welcome to your new Mac.

13. In the Enrollment Actions section, click Add Item.
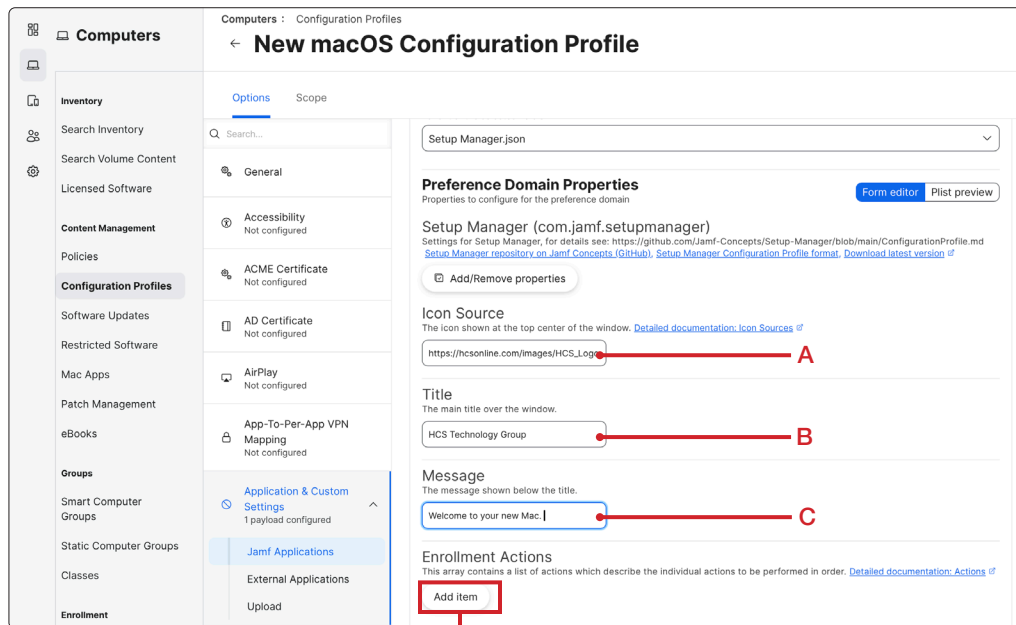
14. For item 1, select Jamf Policy Trigger. Enter the following:
   A. Action Label - The verbiage you want the employee to see when the policy is running in Jamf Setup Manager. This guide will use **Show Me Your ID 3.0**.
   B. Action Icon Source - This can be a URL or a path to an application. This guide will use the URL below.

   https://hcsonline.com/images/HCS_Logo/HCS_Logo_iOS.png

   C. Policy Trigger - Even though the policy has not been created, we are going to name the policy trigger: **install_showmeyourID**.

15. Click Add Item.

16. From the Item 2 menu, select Installomator.

17. Configure the following:
    A. Enter **CodeRunner** in the Action Label Field. NOTE: The Action Label is case sensitive and represents the name of the application being installed by Installomator. You can find a list of Installomator labels in the Labels.txt link below.
    B. The icon can be sourced directly from the CodeRunner page. Use the link below to copy the icon for CodeRunner.
    C. Enter **coderunner** in the Installomator Label field.

    The links provided below explain how Installomator works and the labels Installomator use.
    - Installomator: **https://github.com/Installomator/Installomator**
    - Labels.txt: **https://github.com/Installomator/Installomator/blob/main/Labels.txt**
    - CodeRunner: **https://coderunnerapp.com/images/icon.png**
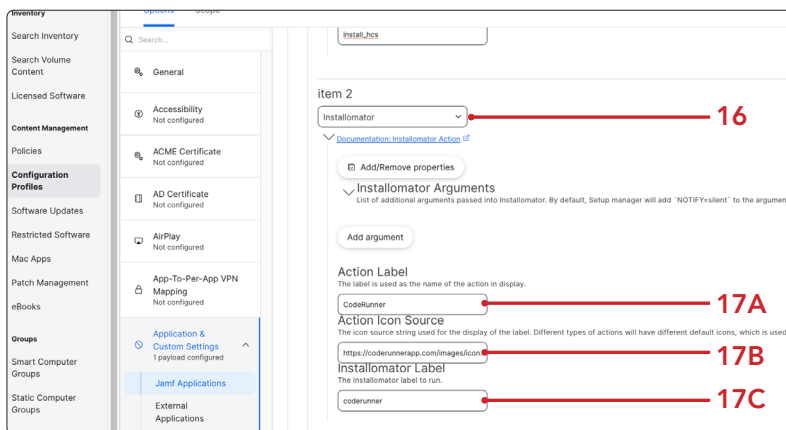
18. Scroll up to Setup Manager (com.jamf.setupmanager). Click Add/Remove properties.

19. Unselect the checkbox for Property. This will clear all entries before selecting the entries listed below. Only Background Image Source, Help Items, and User Data Entry are needed. Select the following from the menu:
    - Enrollment Actions
    - Background Image source
    - Help Items
    - User Data Entry

20. Click Apply.
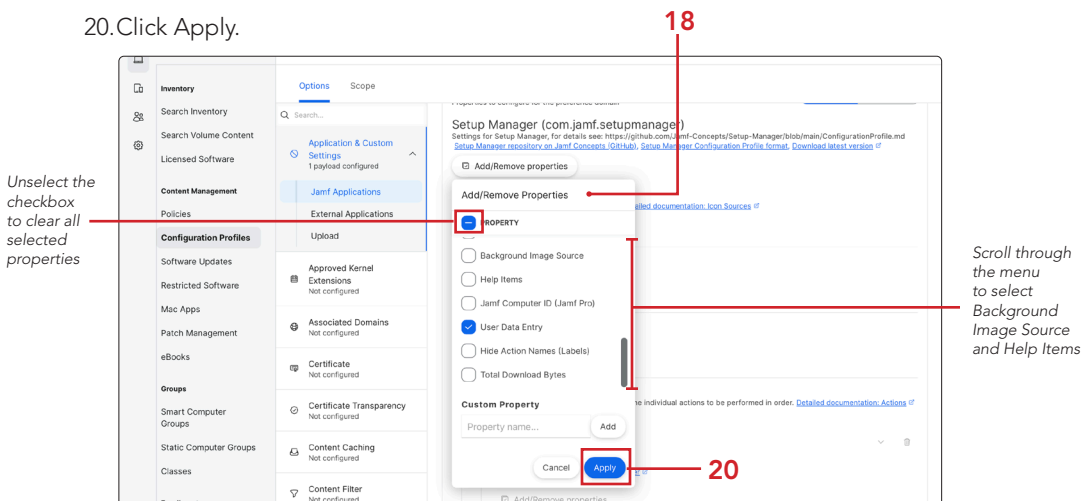
21. Scroll down to User Data Entry. Click Add/Remove Properties.
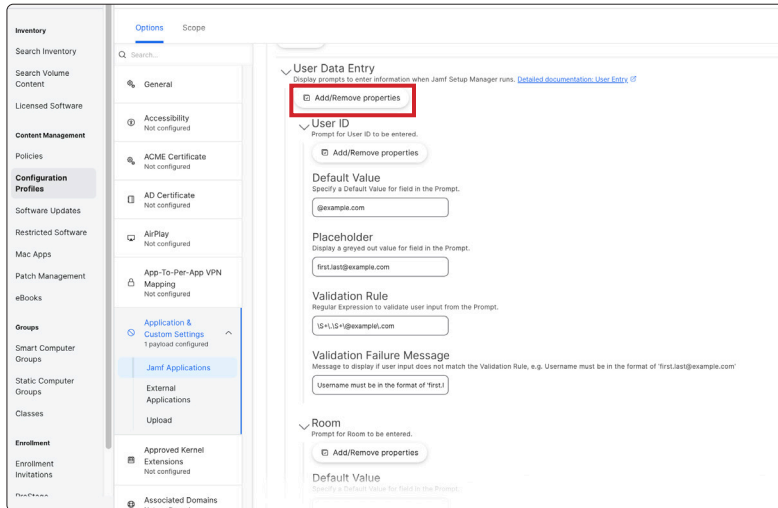
22. Unselect the checkbox for Property. This will clear all entries before selecting the entries listed below. Since this guide will focus on Computer Name and Asset Tag, select the checkboxes for Computer Name and Asset Tag.

23. Click Apply.
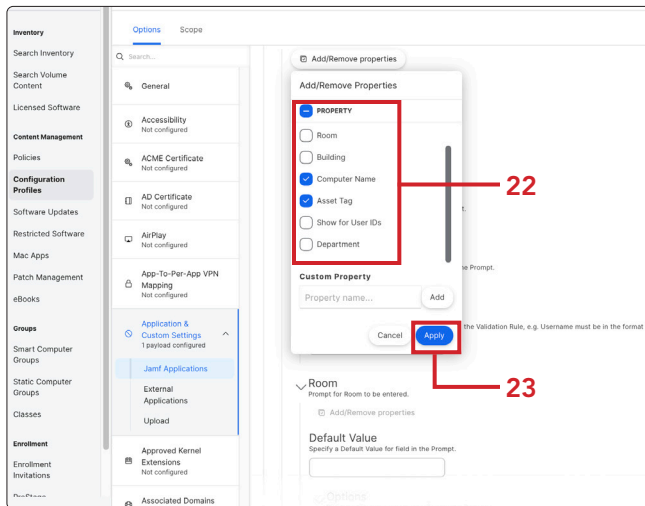
24. Under Computer Name, click Add/Remove properties.

25. Unselect the checkbox for Property. This will clear all entries before selecting the entries listed below. Select the checkbox for Placeholder.

26. Click Apply.
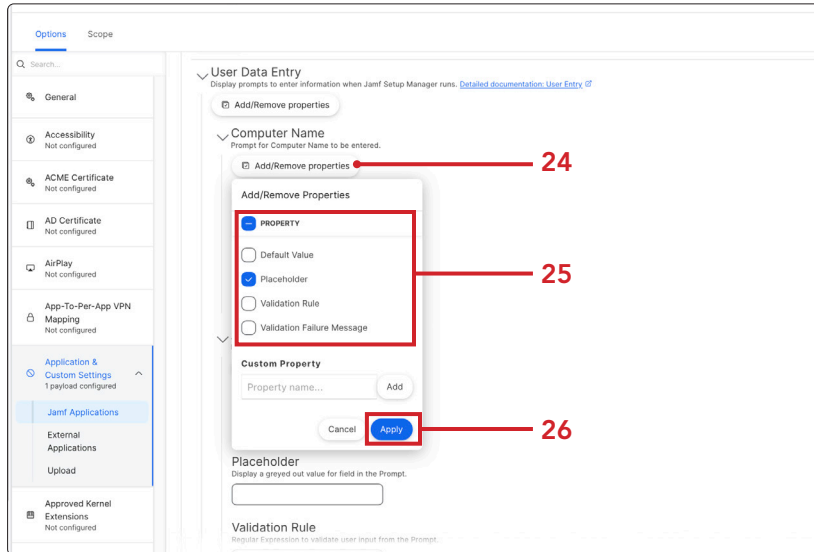
27. In the Placeholder field, enter something you would like to instruct the user to enter. For example "**What is the Macs Serial Number?**"
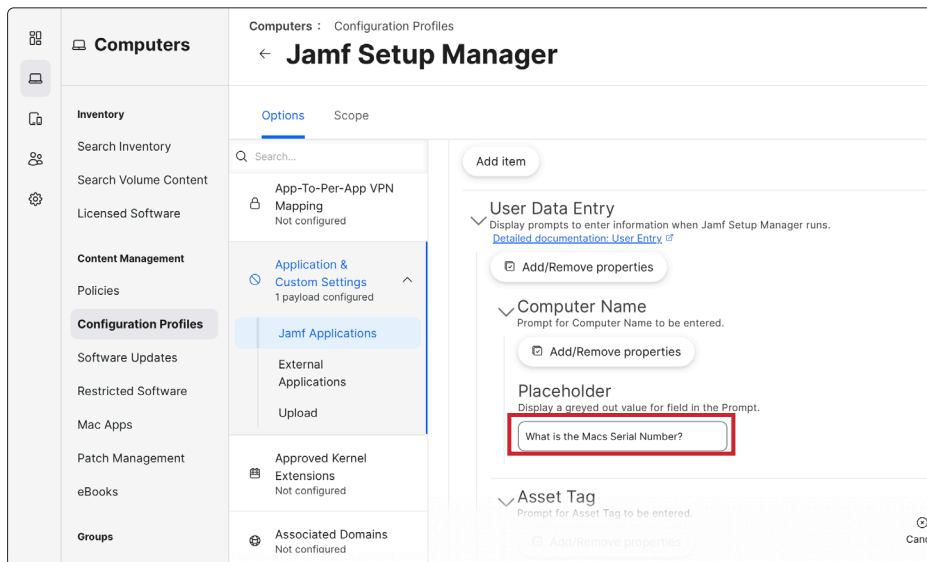
28. Under Asset Tag, click Add/Remove properties.

29. Unselect the checkbox for Property. This will clear all entries before selecting the entries listed below. Select the checkbox for Placeholder.

30. Click Apply.
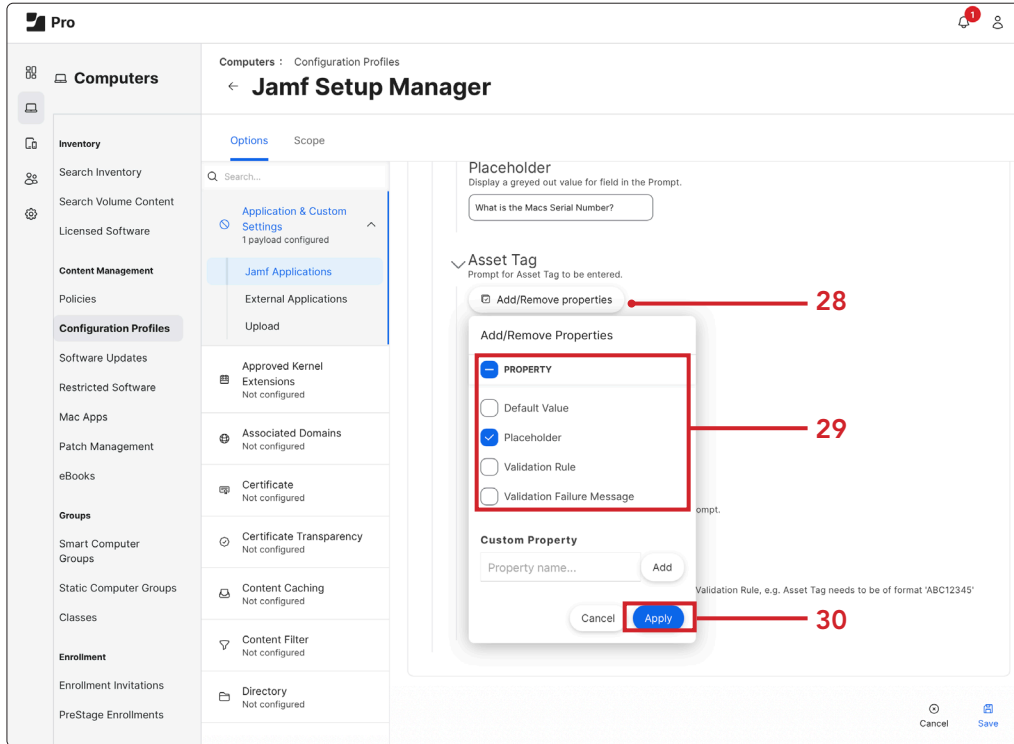
31. In the Asset Tag Placeholder field, enter an asset tag number for your Mac. This guide will use AXXXXX.
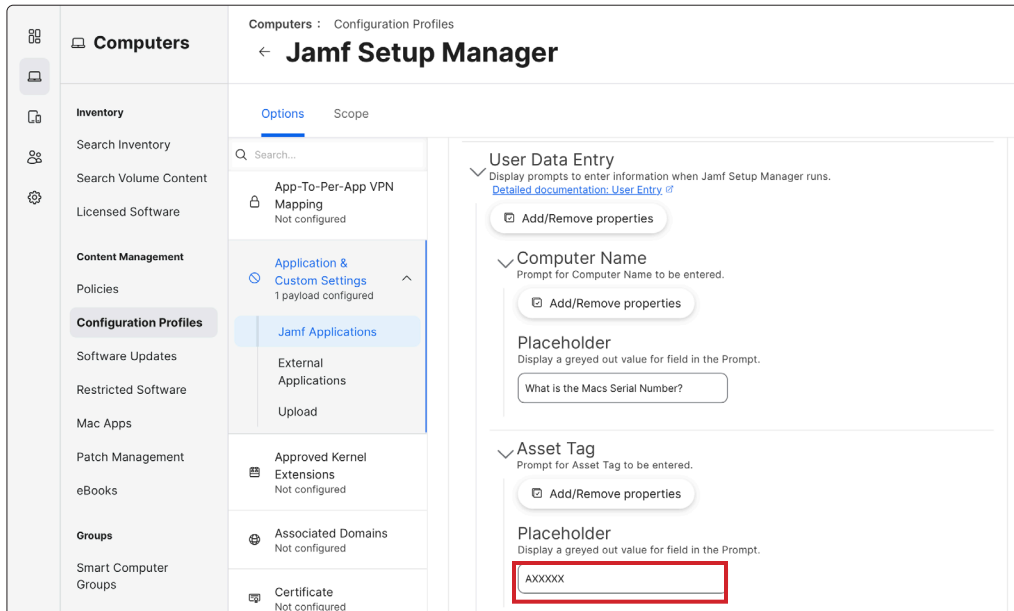
32. Scroll up to Background Image Source. Enter the folowing:
https://hcsonline.com/images/HCS_Logo/Yoda.png

Enter a URL or path from a local Mac
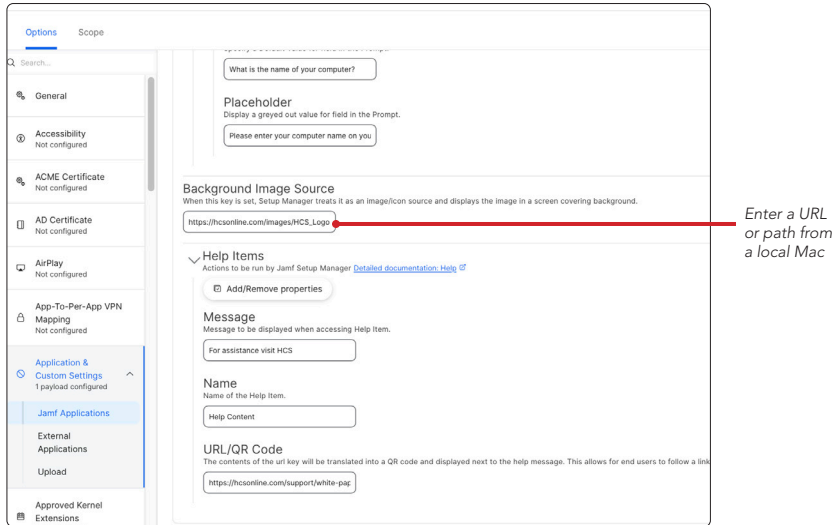
33. Scroll to Help Items. Help Items will help your employees link directly to your support site or to your ticketing system using a QR code.

34. Configure the following:
   A. Message - Visit HCS for more great guides like this
   B. Name - HCS Technology Group
   C. URL/QR code - https://hcsonline.com/support/white-papers
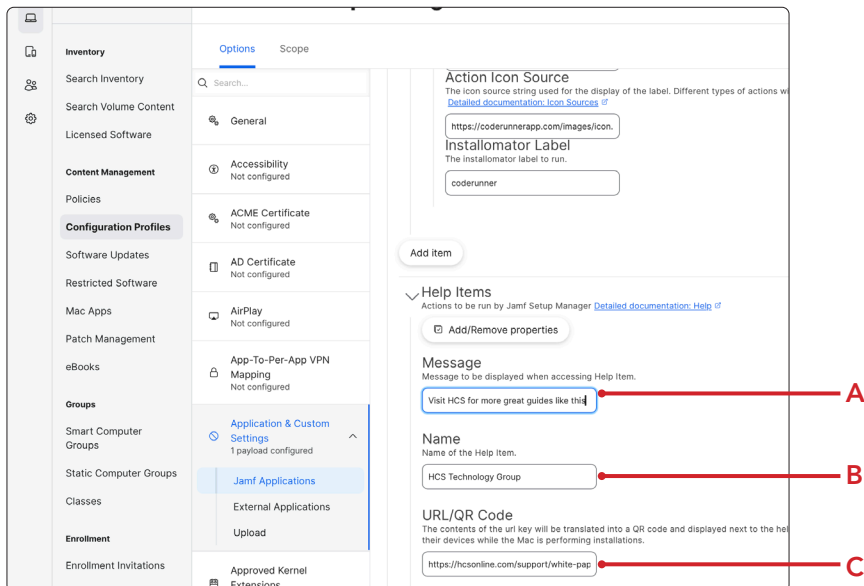
35. Click Scope.

36. Click Add.
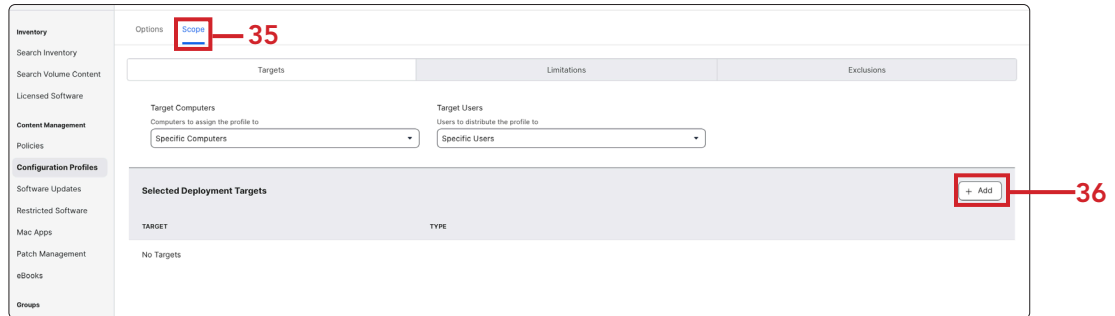
37. Click Computer Groups.

38. Click Add for Macs Enrolled with Jamf Setup Manager PreStage.

39. Click Done.

40. Click Save.

Section 3: Create a Configuration profile for FileVault Enablement

1. Click Configuration Profiles.

2. Click New.
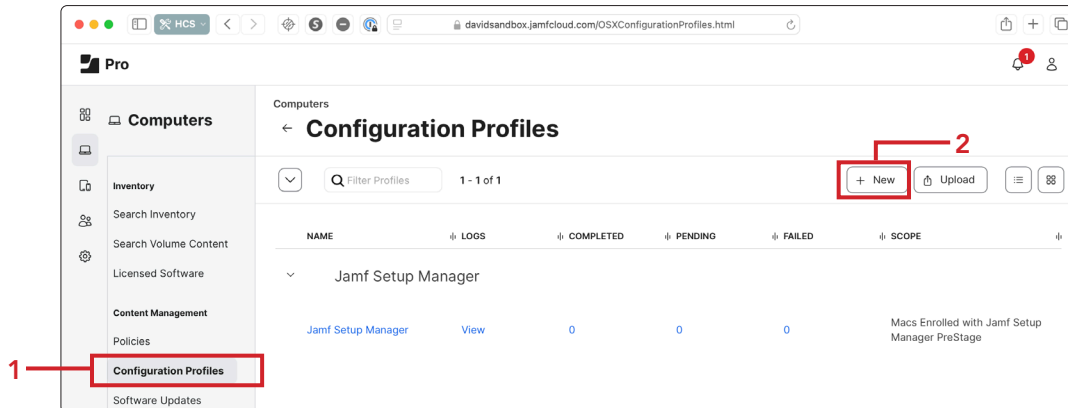
3. In the name field, enter FileVault Enablement for ADE.

4. Select the category, Jamf Setup Manager.
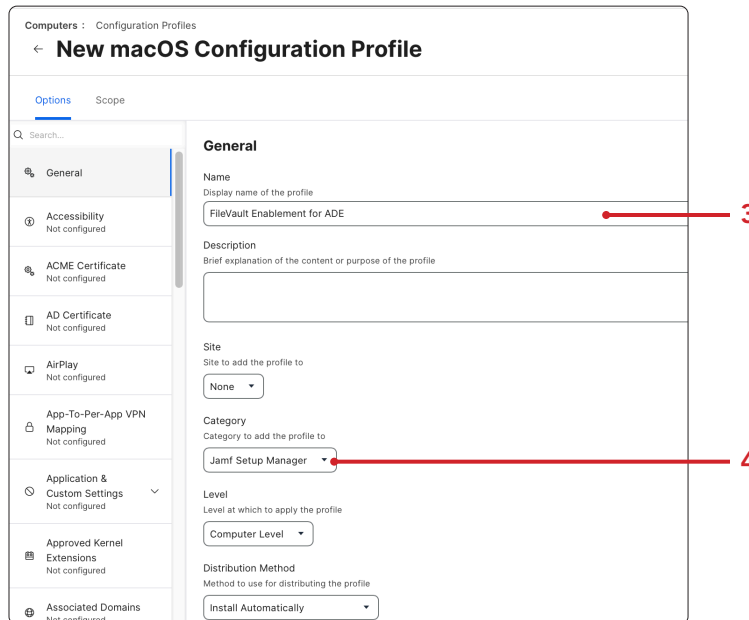
5. Scroll down to the Security and Privacy Payload.

6. Click FileVault.

7. Enable the following:
    A. Enable FileVault
    B. Force Enable in Setup Assistant
    C. Escrow Personal Recovery Key
    D. Enter the following message: **The key will be provided upon request by the IT Dept**.

Configuration Profile

Security and Privacy: FileVault
Settings configured: 4

| Setting | Include |

Enable FileVault — **A**
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 lo... ⌄]

Force Enable In Setup Assistant — **B**
Automatically enable FileVault during user account creation in the Setup Assistant.
ⓘ This setting requires that the configuration profile is installed as part of a PreStage Enrollment.

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

Require user to unlock FileVault after hibernation
When enabled, the user will be required to unlock FileVault when the computer awakes from hibernation
[Disable] [Enable]

Secure Token User Prompt
Determines if the secure token authorization dialog on APFS volumes is bypassed when a mobile account is created. (macOS 10.13.5 or later)
[Hide] [Display]
⚠ When hidden, this may prevent mobile accounts from being able to unlock a FileVault volume

Escrow Personal Recovery Key — **C**
When sent to device, the personal recovery key will be encrypted with the provided certificate and later reported to Jamf Pro. Personal recovery keys that are escrowed can be viewed in the computer's inventory information.

Encryption Method
Method to use for encrypting the personal recovery key. Automatic encryption and decryption is handled by Jamf Pro.
[Automatically encrypt and decrypt recover... ⌄]
ⓘ Jamf Pro automatically generates a required certificate for this encryption method. To see the certificate details, save the profile and navigate to the Certificate payload.

Escrow Location Description
A short location reference to let the end user know where the key will be stored. For example, your organization's name.
[The key will be provided upon request by the IT Dept.] — **D**
Required

"Record Number" Message

8. Click Scope.

9. Click Add.
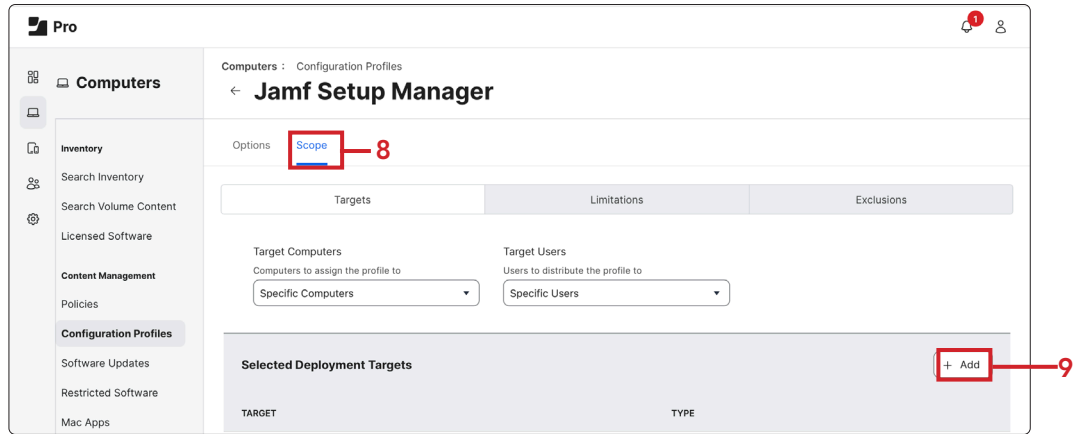
10. Click Computer Groups.

11. Click Add for Macs Enrolled with Jamf Setup Manager PreStage.

12. Click Done.

13. Click Save.

This completes Section 3. In the next section we will create a package with Jamf Composer, upload the package to the Jamf Pro server and create a policy to install the Show Me Your ID 3.0 app.

## Section 4: Create and Deploy a Package file with Jamf Pro

In this section, we will create, upload, and deploy a package using Jamf Pro. Jamf Composer simplifies the process of packaging software for deployment, and Jamf Pro allows us to upload and manage these packages efficiently. We will configure a policy that uses a trigger to automatically install the package on the target macOS devices.

Use Jamf Composer to create a package that contains the application needed for our configuration of Jamf Setup Manager to run during a Mac computer deployment. This guide will NOT cover downloading Jamf Composer from Jamf. It is assumed that Jamf Composer is already installed on your Mac.

1. Open Jamf Composer located in /Applications/Jamf Pro/.

2. Click Cancel.
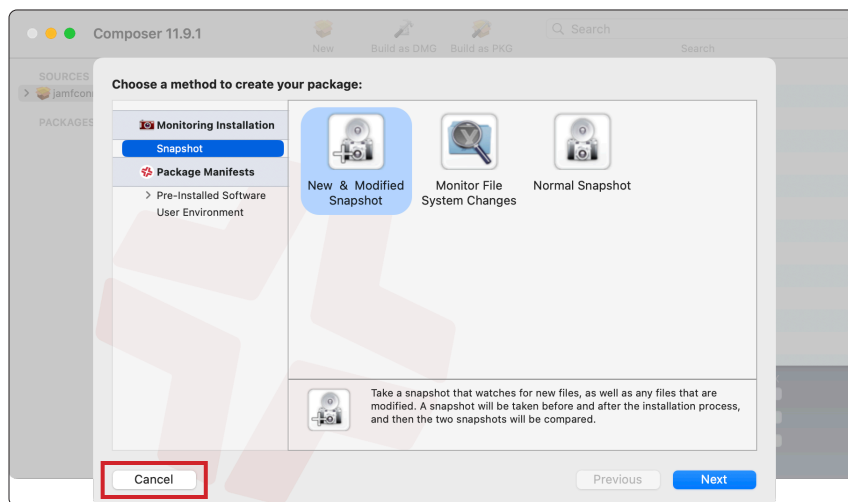
3. Open the Sample Files folder that you downloaded in Section 1 of this guide. Copy the "HCS Show Me Your ID 3.0.app" into the Applications folder on your Mac.

4. Drag and drop the HCS Show Me You ID 3.0.app to the Sources section in Jamf Composer. You will see a green plus sign indicating the file will be copied into Jamf Composer.
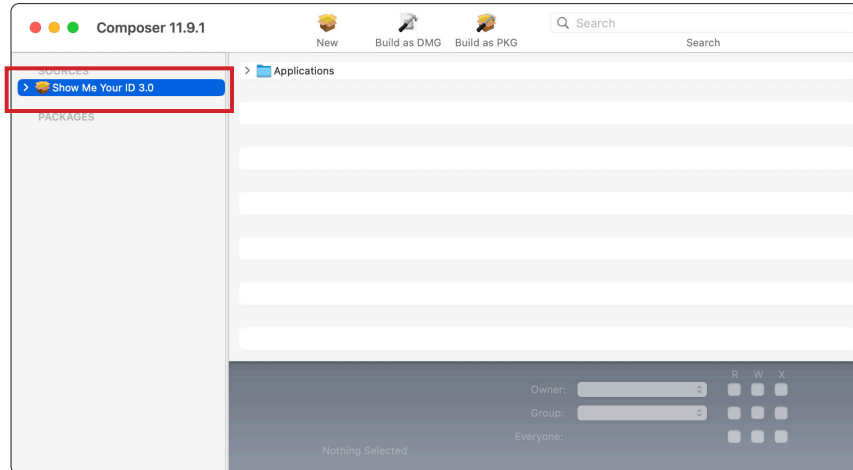
5. After the file is copied, confirm Show Me Your ID 3.0 is under Sources.

6. Expand the folder Applications.

7. Select Show Me Your ID 3.0.app to verify the permissions.

8. Set the permissions to:
    A. Owner: Root (R-W-X)
    B. Group: Wheel (R- -X)
    C. Everyone (R- -X)
    D. Click "Build as PKG" (This will ask for the admin credentials of the Mac.)
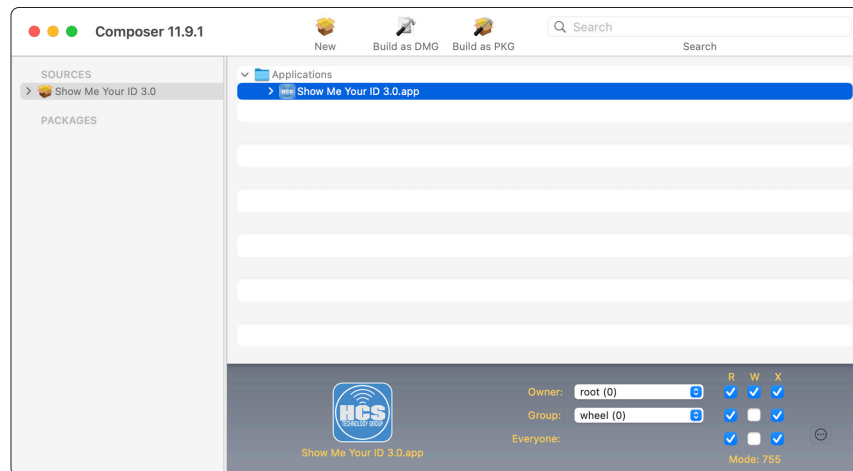
9. Save the package to your Desktop.
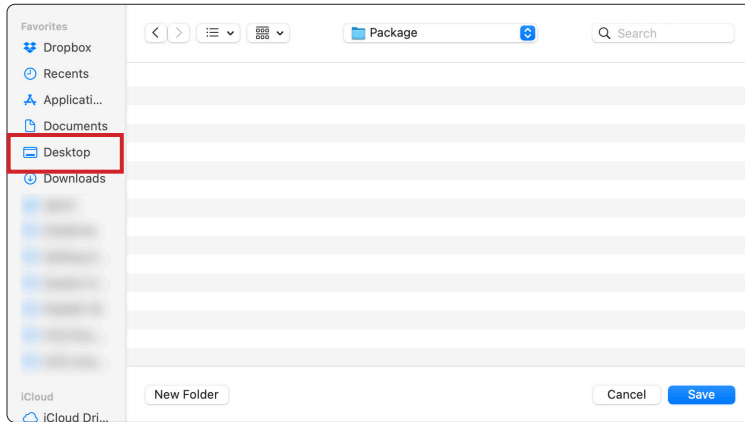
10. Rename the package to ShowMeYourID3.pkg. We are renaming the package to remove any space from the package name.
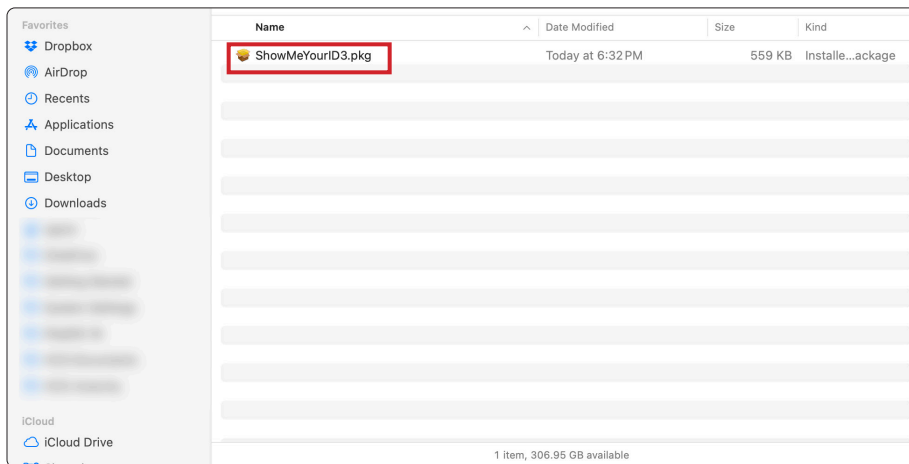
Section 5: Upload Packages to Jamf Pro

1. Go back to your Jamf Pro Server.

2. Click Settings.

3. Click Computer management.

4. Click Packages.

5. Click New.

6. Drag the Setup.Manager.1.0-368.pkg from your Downloads folder to the "Drop file here" field.

7. Set the Category to Jamf Setup Manager.

8. Click Save.

9. Click Previous (←).

10. Click New.

11. Repeat steps 6 through 9 for upload ShowMeYourID3.pkg.

12. Confirm you have uploaded the following packages before continuing:
   • Setup.Manager.1.0-368.pkg
   • ShowMeYourID3.pkg

Section 6: Create a Policy in Jamf Pro

1. Click Computers.

2. Click Policies.

3. Click New.
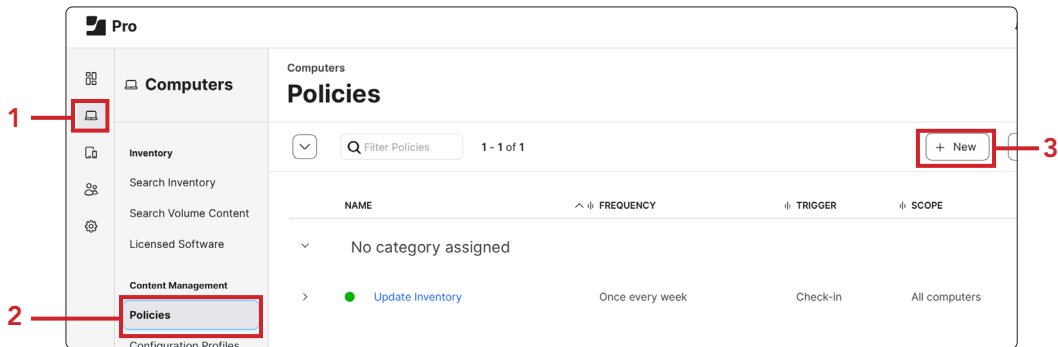
4. Configure the following:
   A. Display Name: **HCS Show Me Your ID 3.0**
   B. Category: Select a category of your choosing. This guide will use Jamf Setup Manager
   C. Trigger: Select Custom and enter **install_showmeyourID**
   D. Execution Frequency: Ongoing
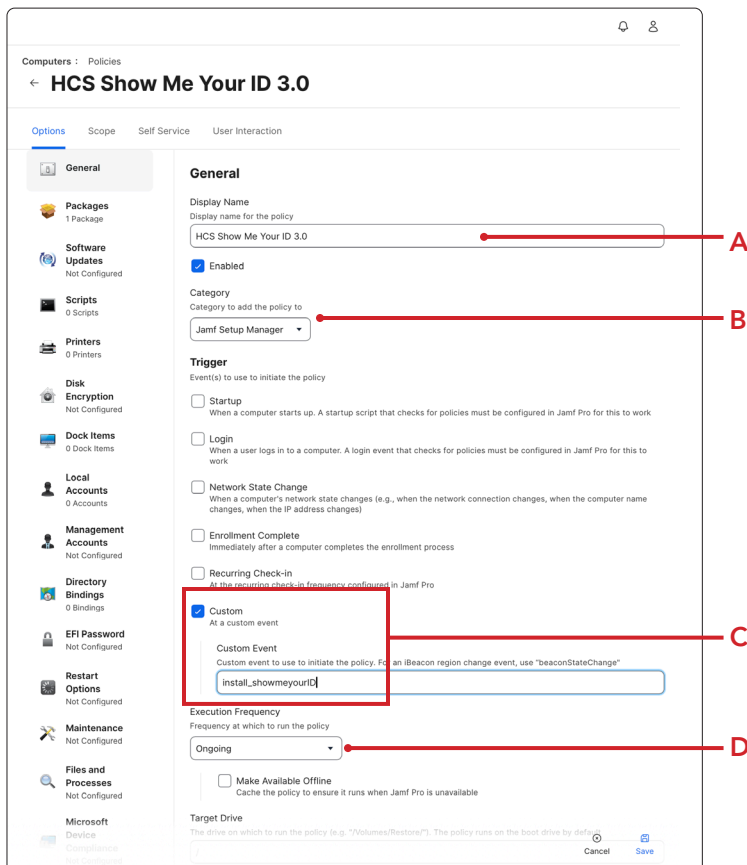
5. Click the Packages payload.

6. Click Configure.
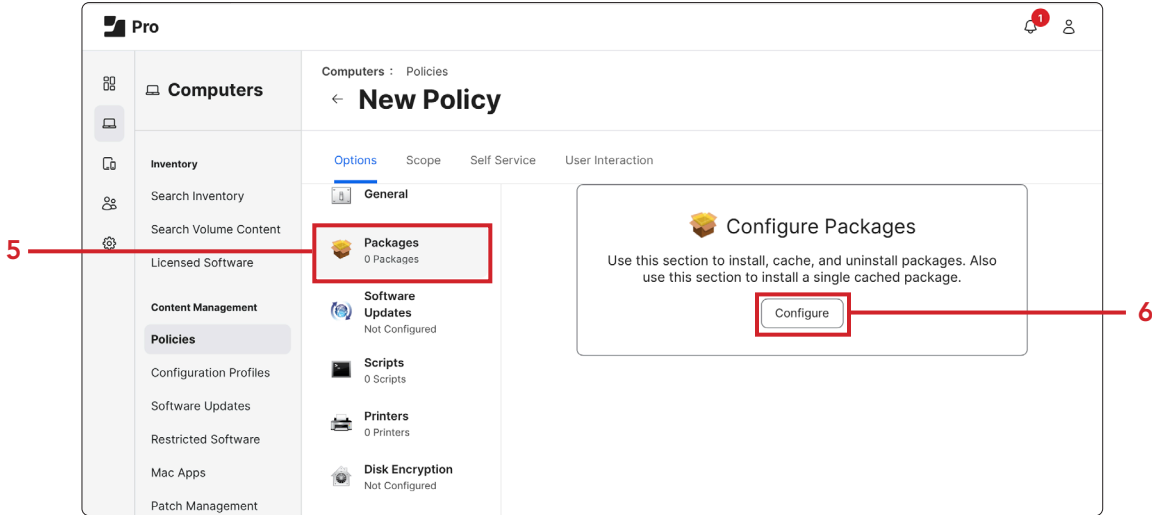
7. Click add for ShowMeYourID3.pkg.
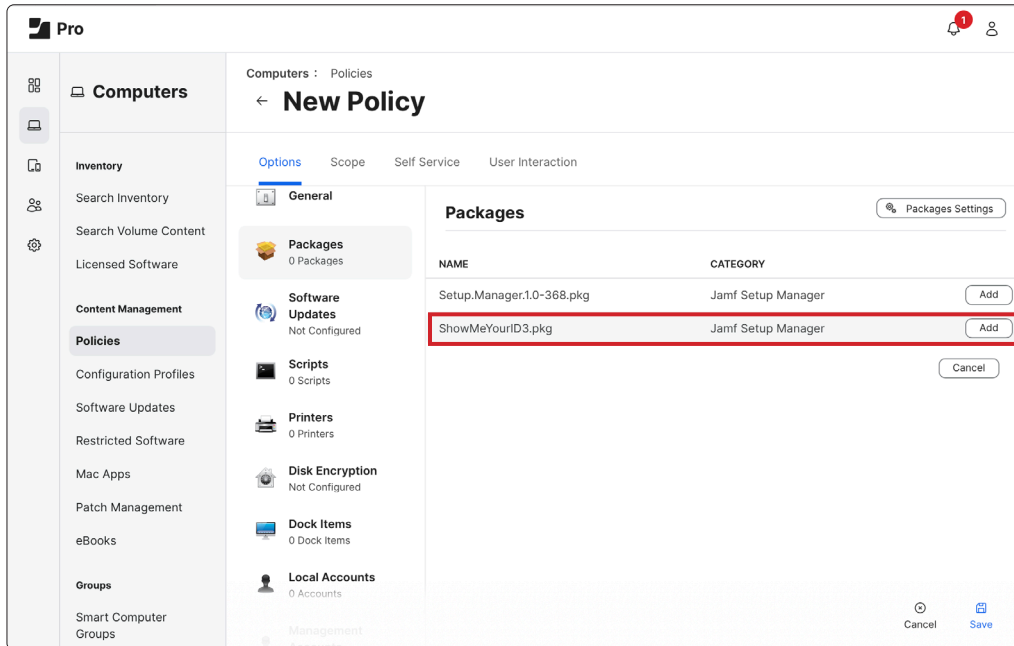
8. Confirm the action is set to install.

9. Click Scope.

10. Click Add.

11. Click Computer Groups.

12. Click Add for Macs Enrolled with Jamf Setup Manager PreStage.

13. Click Done.
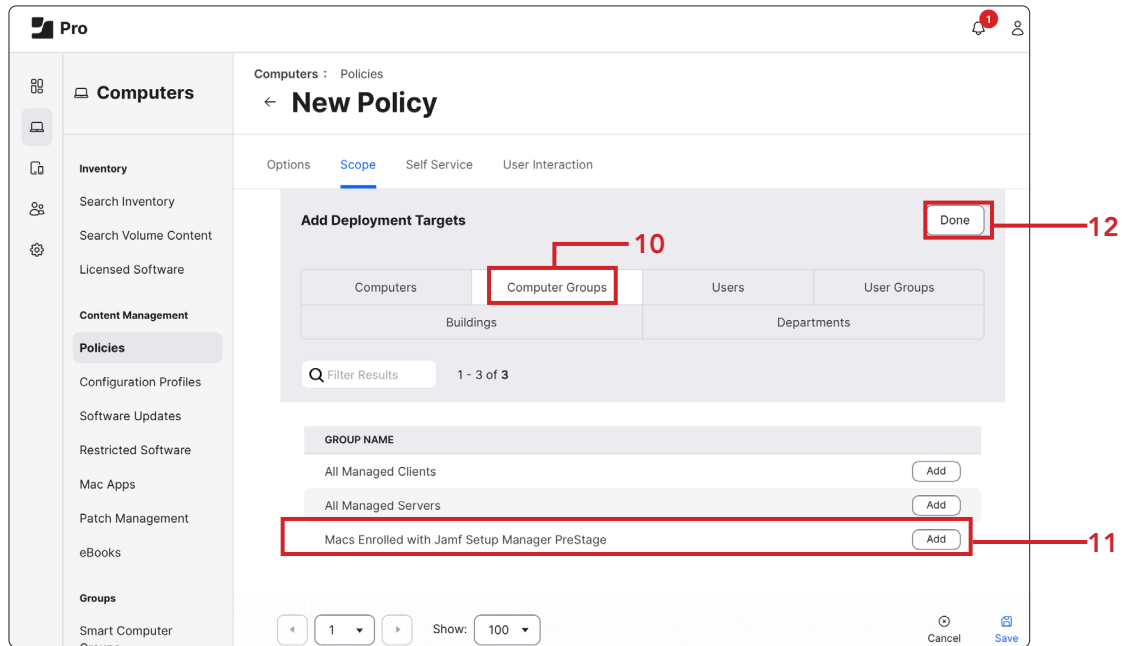
14. Click Save.
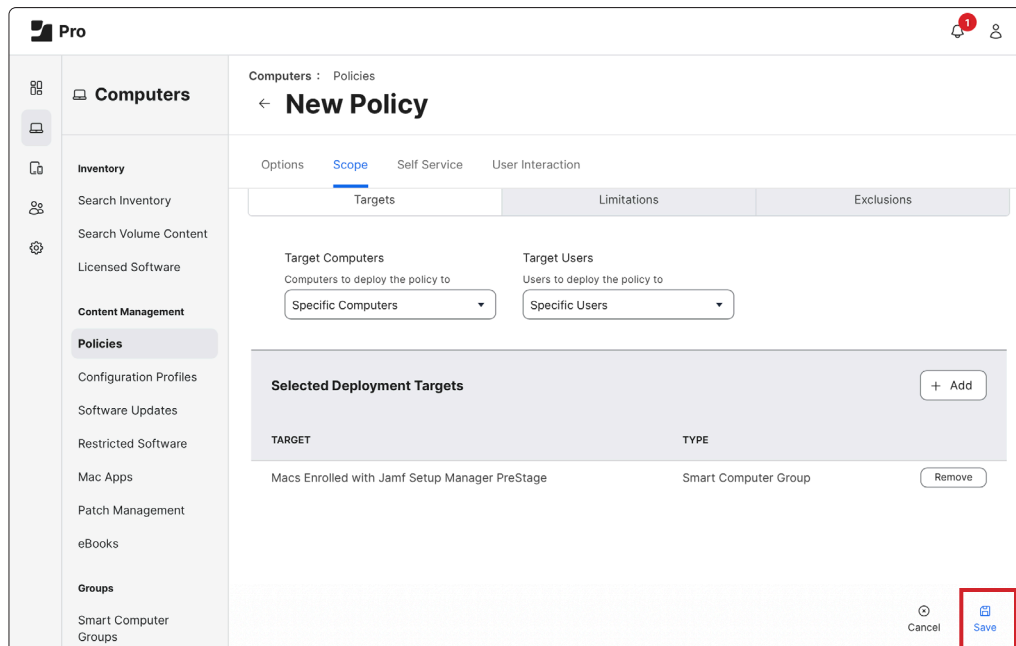
15. Confirm the policy was created.

This completes section 6. In the next section, we will create the PreStage enrollment, configure all components, demonstrate how the macOS minimum required version and FileVault forced Enablement works alongside Jamf Setup Manager, and test the entire setup.

Section 7: Configure the PreStage Enrollment using Jamf Setup Manager

In this section, we will finalize the setup by editing the PreStage enrollment from Section 1 and configuring all necessary settings. We will demonstrate how the minimum macOS version requirement is enforced during the enrollment process with Jamf Setup Manager, as well as ensure FileVault is automatically enabled. We will test the entire workflow to verify everything functions as expected, including PreStage enrollment, package deployment, macOS version compliance, and FileVault enablement.

The minimum macOS version feature in Jamf Pro 11.9 requires macOS 14.4 or later. This guide is using macOS 14.5. If you're not using 14.4 or later, this feature will be skipped during setup assistant.

1. Click Computers.

2. Click PreStage Enrollments.

3. Click on Jamf Setup Manager.
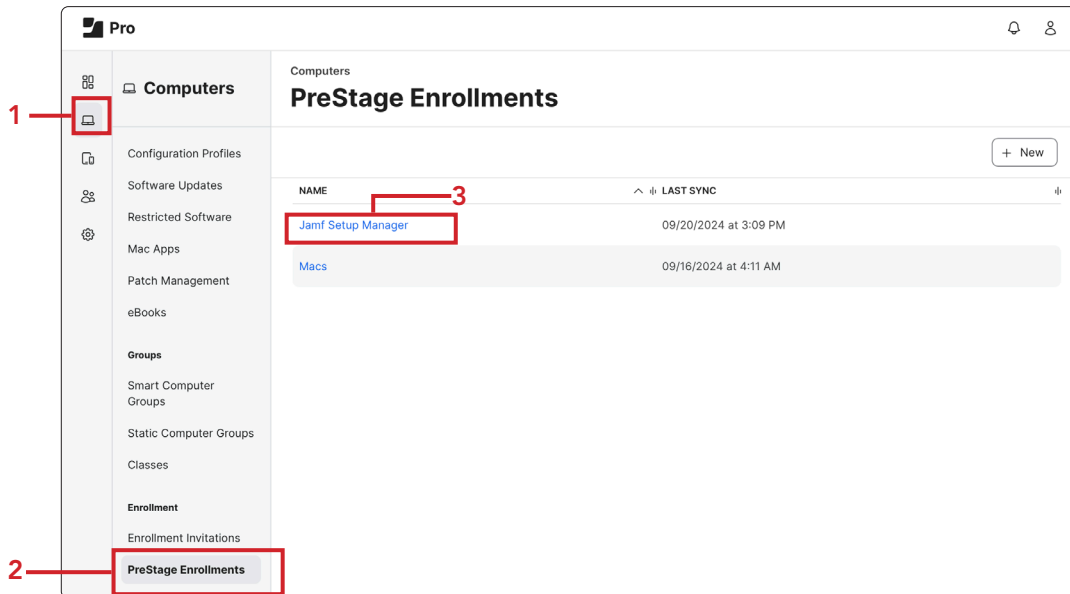
This guide will only focus on configuring the minimum required macOS Version, FileVault Enablement, Configuration Profiles and Enrollment packages.

4. On the bottom-right, click Edit.
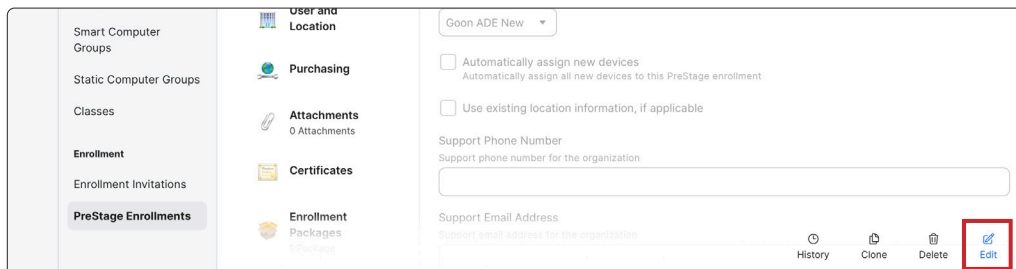
5. In the General payload, scroll down to Minimum required macOS version.

6. From the menu, select "Latest version based on computer eligibility". This will verify that the device is on the latest macOS based on Mac eligibility before going through Automated Device Enrollment. NOTE: The minimum macOS version requirement for this feature is macOS 14.4 or later.
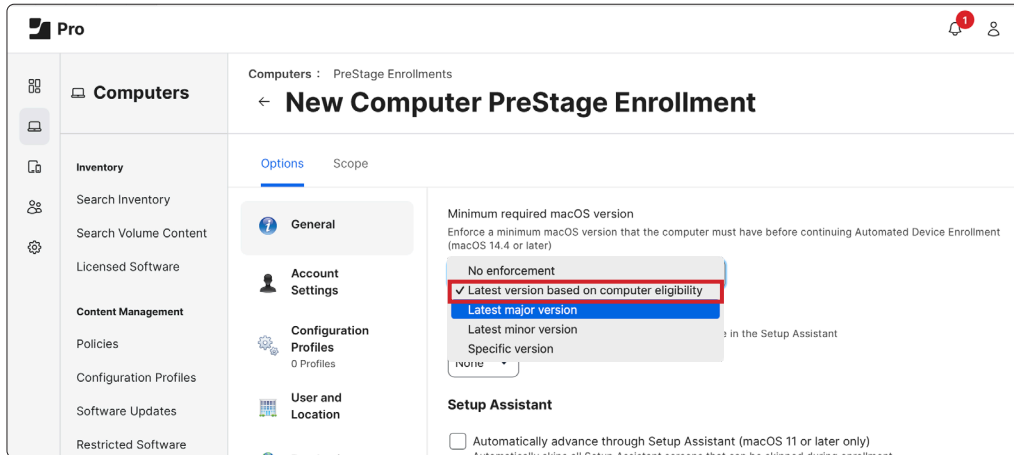
7. Scroll down to Setup Assistant Options, click All to select everything.

8. Deselect the box for Location Services and FileVault. We'll leave these unselected so FileVault will automatically enable with a configuration profile during the setup and the user will be prompted to enable Location Services during setup assistant.
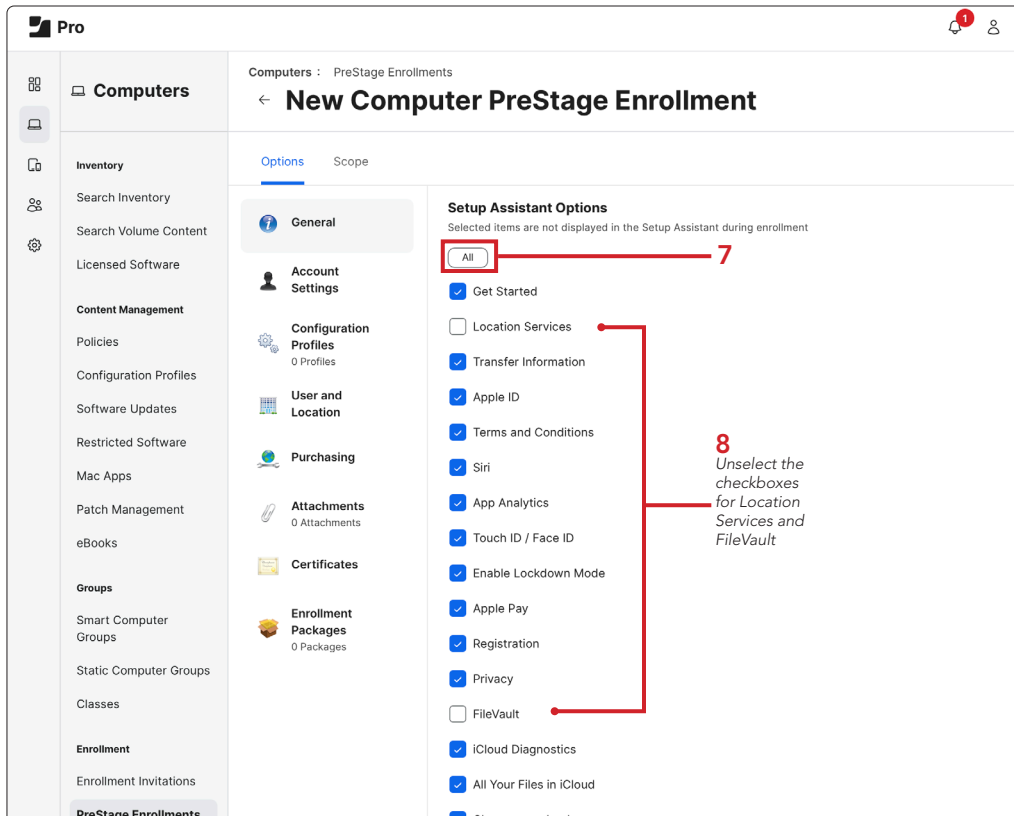
9. Click on the Configuration Profile payload.

10. Click Configure.

11. Select FileVault Enablement for ADE and Jamf Setup Manager profile.

12. Click Enrollment Packages.

13. Click Configure.

14. Click Add for Setup.Manager.1.0-368.pkg.

15. Select the radio button for Cloud Distribution Point (Jamf Cloud.)

16. Click Scope.

17. Select a Mac to use for testing with Jamf Setup Manager.

18. Click Save.

Section 8: Enrolling and testing Jamf Setup Manager

Now we are ready to enroll a device and see Jamf Setup Manager in action.

1. Power on your Mac computer and follow the on screen instructions. When you get to the Remote Management screen, Click Enroll and continue to follow the on screen instructions. Jamf Setup Manager will start once the the device goes past the remote management screen.
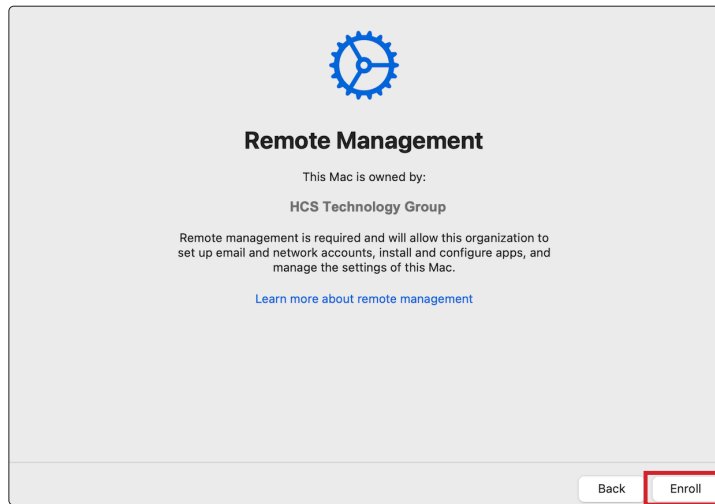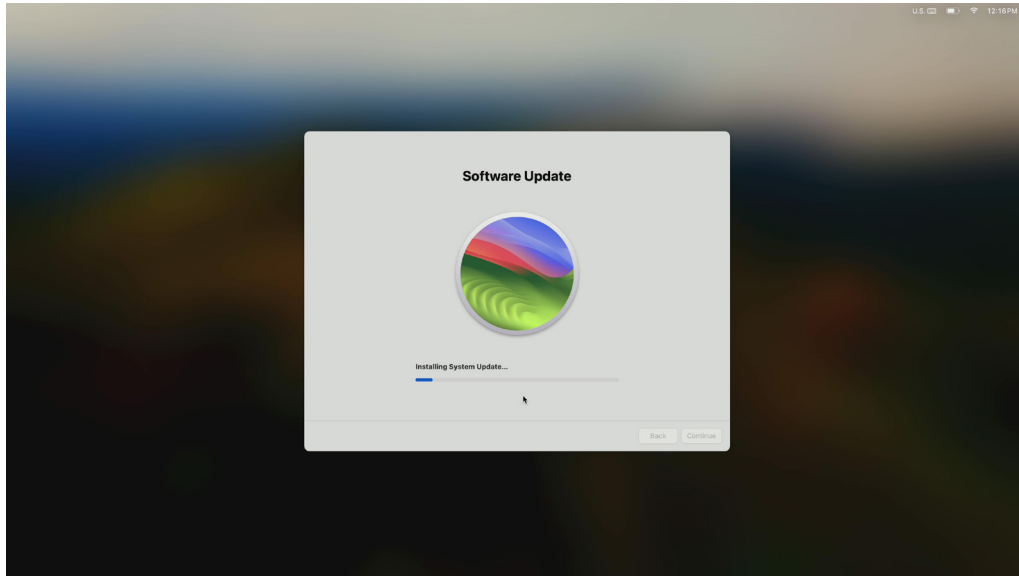

2. Since we configured the Minimum required macOS Version we will see the following screen. Click Continue.
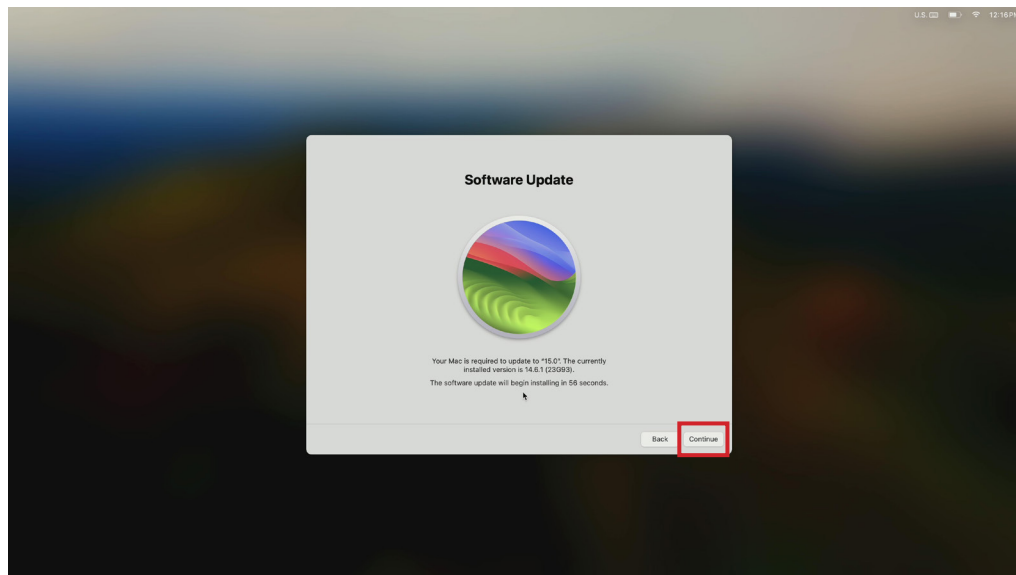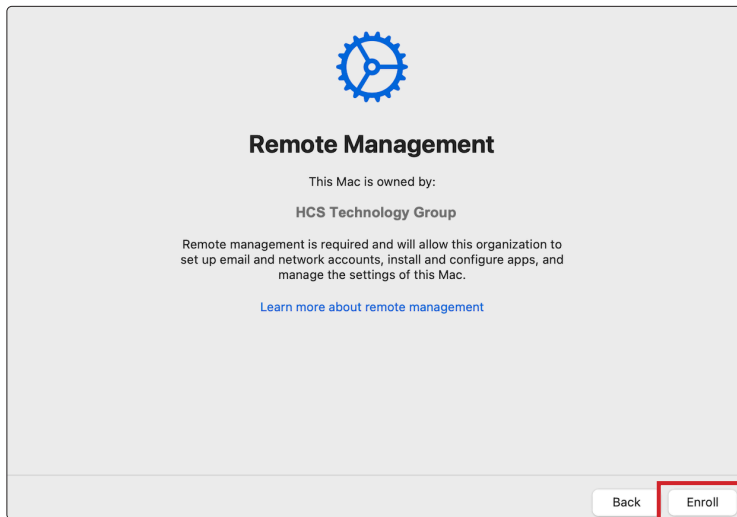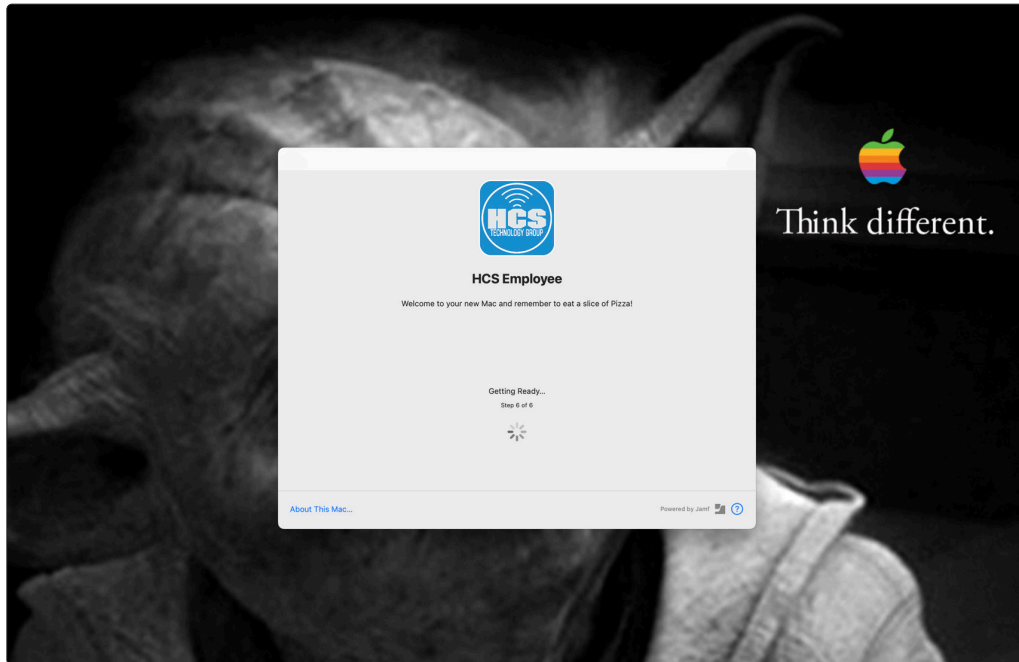
3. The macOS update will begin.

4. The Mac will restart once this process is finished and the remote management screen will once again appear and ask to enroll the device.
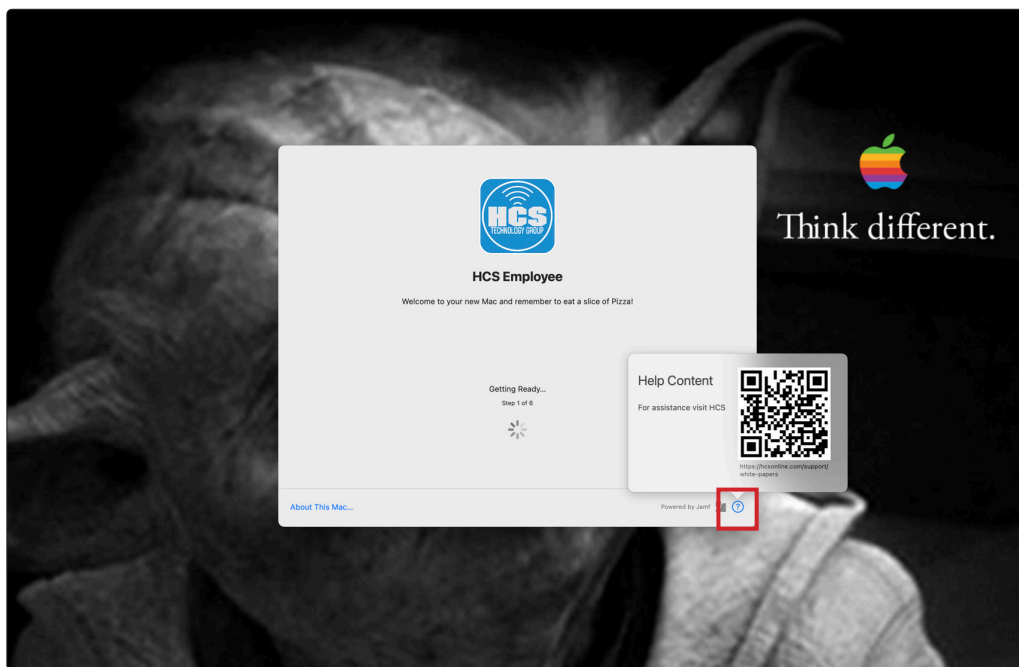
5. Click Enroll

6. The Jamf Setup Manager process will begin. Provisioning will start when steps 1-6 are completed.
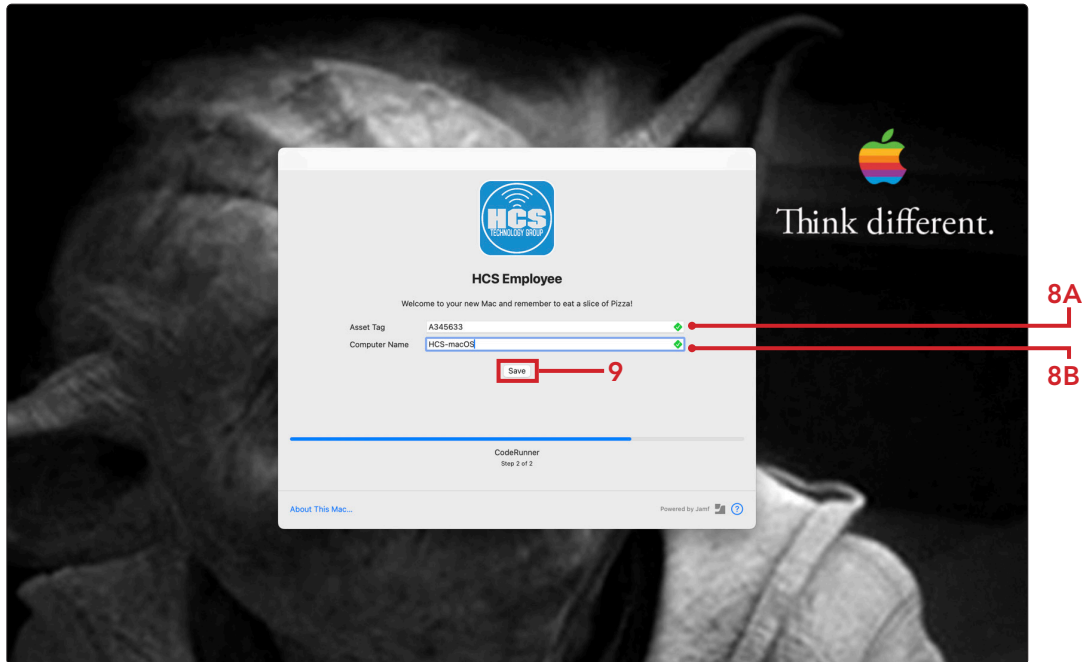

7. Click Help (⑦) to display the QR code. This will take to the website we configured earlier in this guide.
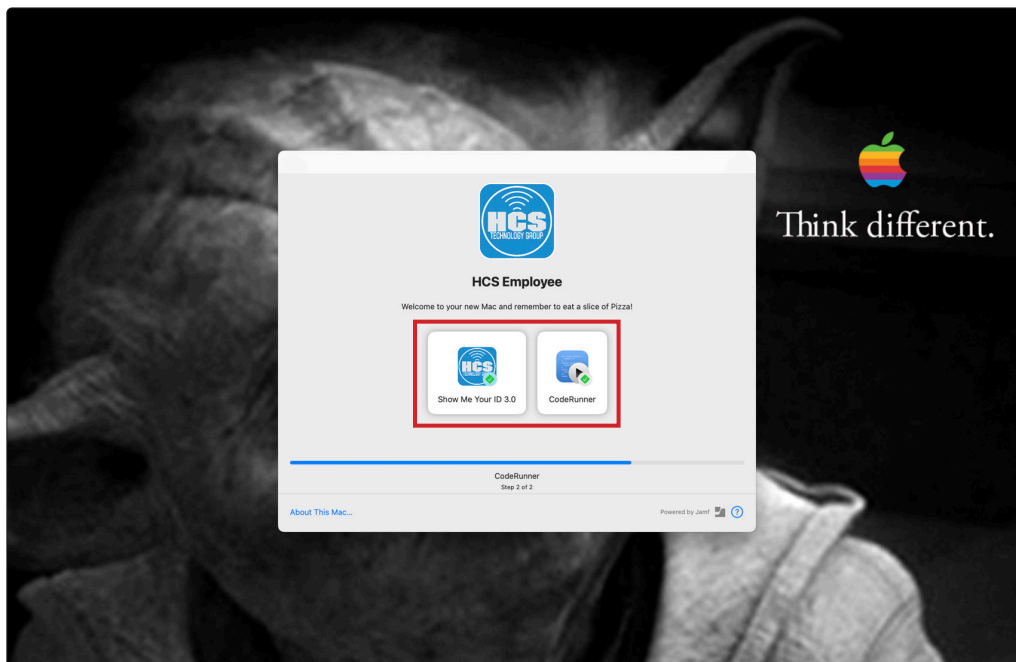
8. Configure the following:
   A. Asset Tag - Enter your asset tag
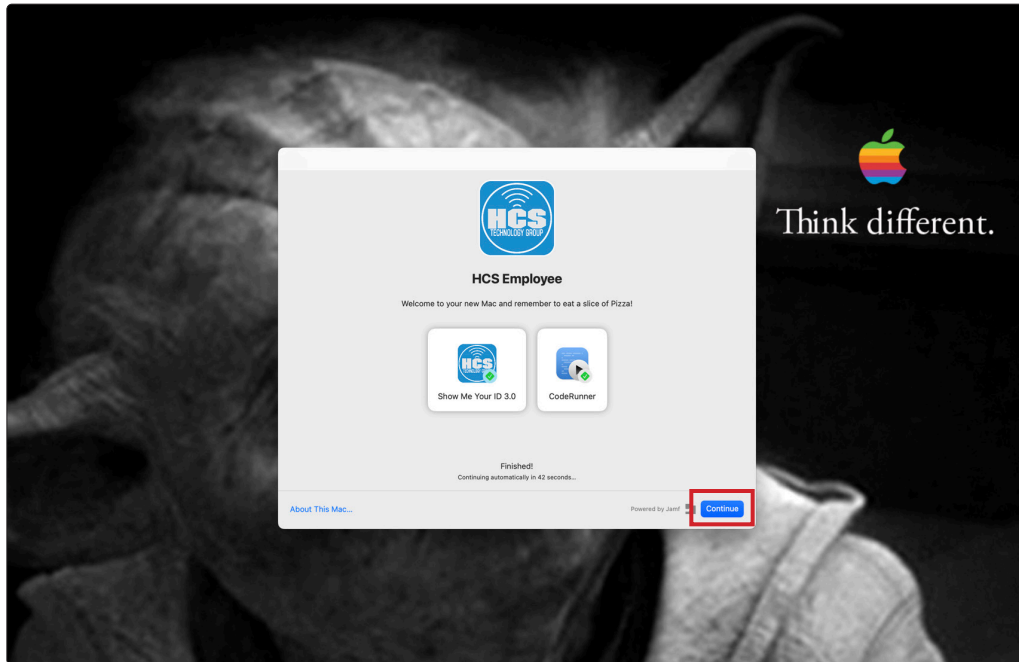   B. Computer Name - Enter your computer name

9. Click Save.

10. Confirm that Show Me Your ID 3.0 and CodeRunner apps are installing.
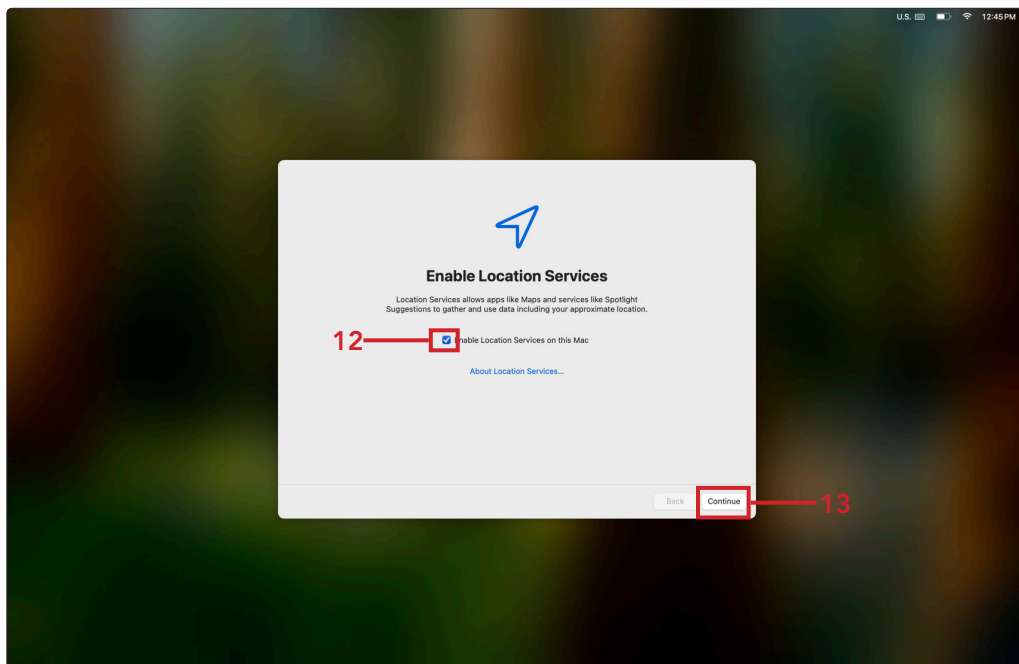
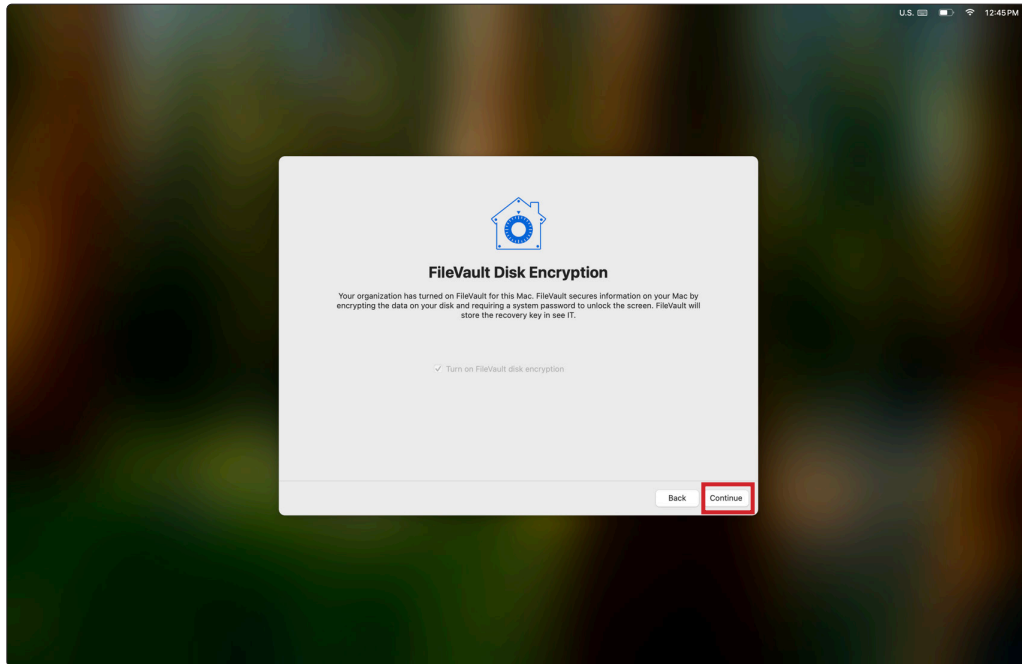11. Jamf Setup Manager is complete. Click Continue.

12. Enable Location Services.

13. Click Continue.

14. Confirm the FileVault Disk Encryption appears and has been enabled. Click Continue.
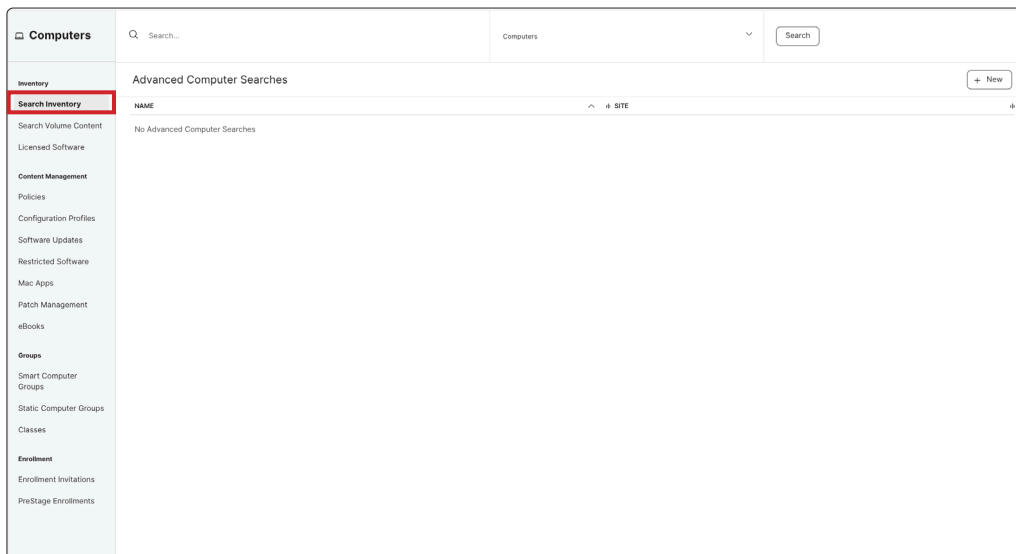

15. Create a user account.

16. The Mac was enrolled successfully in Jamf Pro.

17. Go back to your Jamf Pro Server.

18. Click on Computers.

19. Click Search Inventory.

20. Search for the name of the computer that you named in Step 8.

21. Click on the Computer name:
    A. General Tab you will see that the device is named as it was in the example: HCS-macOS
    B. Scroll down to view the Asset Tag.

Jamf Setup Manager: Logs

- /Library/Logs/Setup Manager.log - These logs provide valuable insight into the actions performed during the setup process, including software installations, configuration changes, and any potential issues encountered during Jamf Setup Manager. Administrators can use this log file for troubleshooting, verifying that setup tasks completed successfully, and ensuring that policies such as installomator installations, app deployments, and branding have been applied correctly.

This completes the guide.