

Deploying macOS 10.7-10.12.6 with Jamf Pro

Technical Paper
Jamf Pro 9.21 or Later
11 March 2019

© copyright 2002-2019 Jamf. All rights reserved.

Jamf has made all efforts to ensure that this guide is accurate.

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Apple, the Apple logo, FileVault, FireWire, Mac, macOS, and OS X are trademarks of Apple Inc., registered in the U.S. and other countries. The App Store is a service mark of Apple Inc., registered in the U.S. and other countries

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, Jamf, the Jamf Logo, JAMF SOFTWARE®, the JAMF SOFTWARE Logo®, RECON®, and the RECON Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

Contents

4 Introduction

- 4 What's in This Guide
- 4 Additional Resources

5 Overview

6 Deploying a macOS Upgrade

- 6 Requirements
- 7 Step 1: Add the .app File for macOS to Jamf Admin
- 8 Step 2: Cache the InstallESD.dmg File
- 10 Step 3: Create a Smart Computer Group
- 11 Step 4: Create a Self Service Policy for Upgrading macOS

15 Deploying macOS by Imaging

- 15 Requirements
- 15 Step 1: Prepare to Image a Partition
- 19 Step 2: Image Computers

21 Revision History

Introduction

What's in This Guide

This guide provides step-by-step instructions on how to deploy macOS 10.7-10.12.6 with Jamf Pro.

Additional Resources

For more information on Jamf Pro-related topics, see the [*Jamf Pro Administrator's Guide*](#).

Overview

This guide provides workflows for two different macOS deployment scenarios:

- **Deploying a macOS upgrade**—This should be used for upgrading macOS on computers that are already configured in your environment. It allows you to preserve the settings and files on computers. For instructions, see [Deploying a macOS Upgrade](#).
- **Deploying macOS by imaging**—This should be used for configuring newly purchased computers or re-purposing computers that are already part of your environment. It gives you complete control over the settings and files on computers. For instructions, see [Deploying macOS by Imaging](#).

Deploying a macOS Upgrade

Deploying macOS 10.7-10.12.6 as an upgrade involves the following steps:

1. Add the .app file for macOS to Jamf Admin.
2. Cache the `InstallESD.dmg` file using a policy.
3. Create a smart computer group.
4. Create a Self Service policy for upgrading macOS.

Note: The name of the `InstallESD.dmg` file in Jamf Admin will vary depending on the version of macOS that you plan to deploy. For example, the name of the `InstallESD.dmg` file for OS X 10.10 would be `Install OS X Yosemite.InstallESD.dmg`.

Requirements

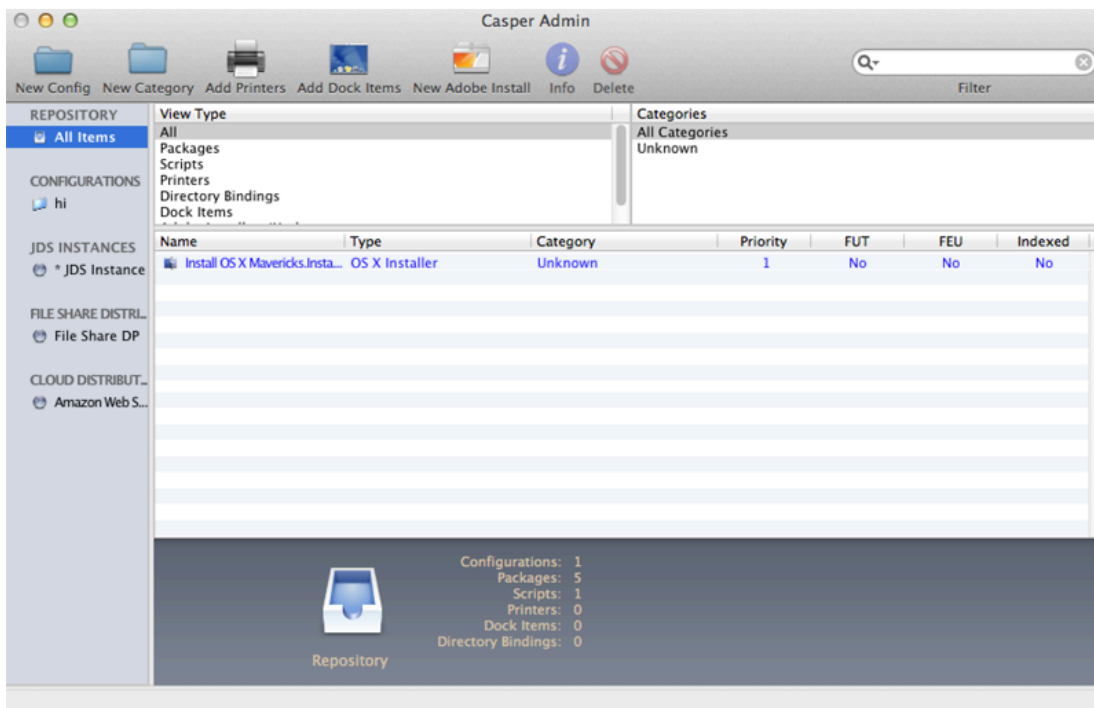
- Jamf Pro 9.21 or later
Note: If you are using Jamf Pro 8.3-9.1, see the [Deploying macOS 10.7 or Later with Jamf Pro](#) Knowledge Base article for instructions on deploying a macOS upgrade.
- Jamf Admin
- The .app file for the version of macOS that you plan to deploy (For example, `Install OS X Mountain Lion.app`.)
You can obtain the latest .app file for macOS from the Mac App Store.
- Managed computers with:
 - (For deployments of macOS 10.10 or later only) macOS 10.7 or later
Computers with macOS 10.5 or macOS 10.6 must be upgraded to macOS 10.7 or later before upgrading to macOS 10.10.
 - Self Service
 - The system requirements for the version of macOS that you plan to deploy
 - macOS 10.7: <http://support.apple.com/kb/HT4949>
 - macOS 10.8: <http://support.apple.com/kb/HT5444>
 - macOS 10.9: <http://support.apple.com/kb/HT5842>
 - macOS 10.11: https://support.apple.com/kb/SP728?locale=en_US
 - macOS 10.12: <https://support.apple.com/en-us/HT201475>

Step 1: Add the .app File for macOS to Jamf Admin

Add the .app file for macOS to Jamf Admin. Jamf Admin extracts the `InstallESD.dmg` file from the .app file so you can cache and install it using policies.

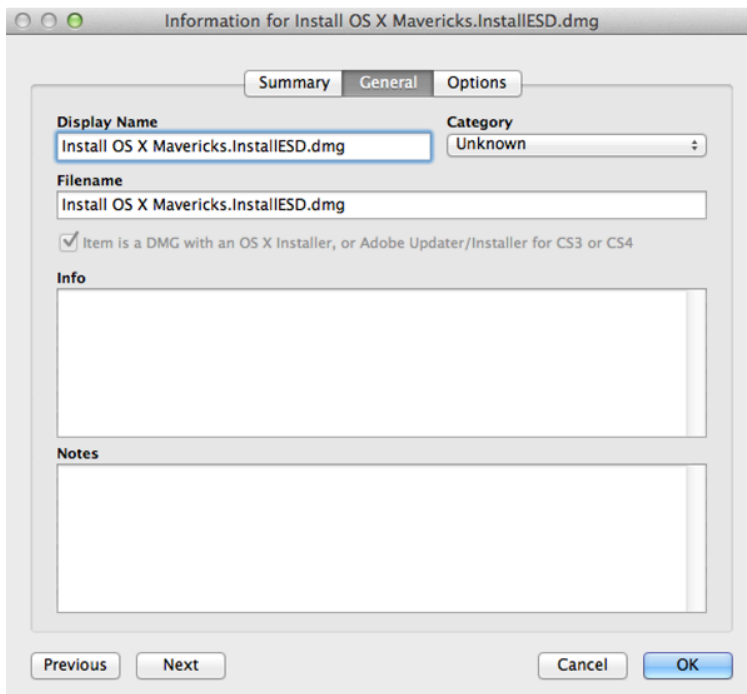
1. Open Jamf Admin and authenticate to the Jamf Pro server.
2. Drag the .app file to the main repository in Jamf Admin.
Jamf Admin extracts the `InstallESD.dmg` file, analyzes its contents, and adds it to the master distribution point and Jamf Pro.

The `InstallESD.dmg` file is displayed in blue text until you add it to a category.



3. Double-click the package in the main repository.


4. Click the **General** tab and choose a category for the package.



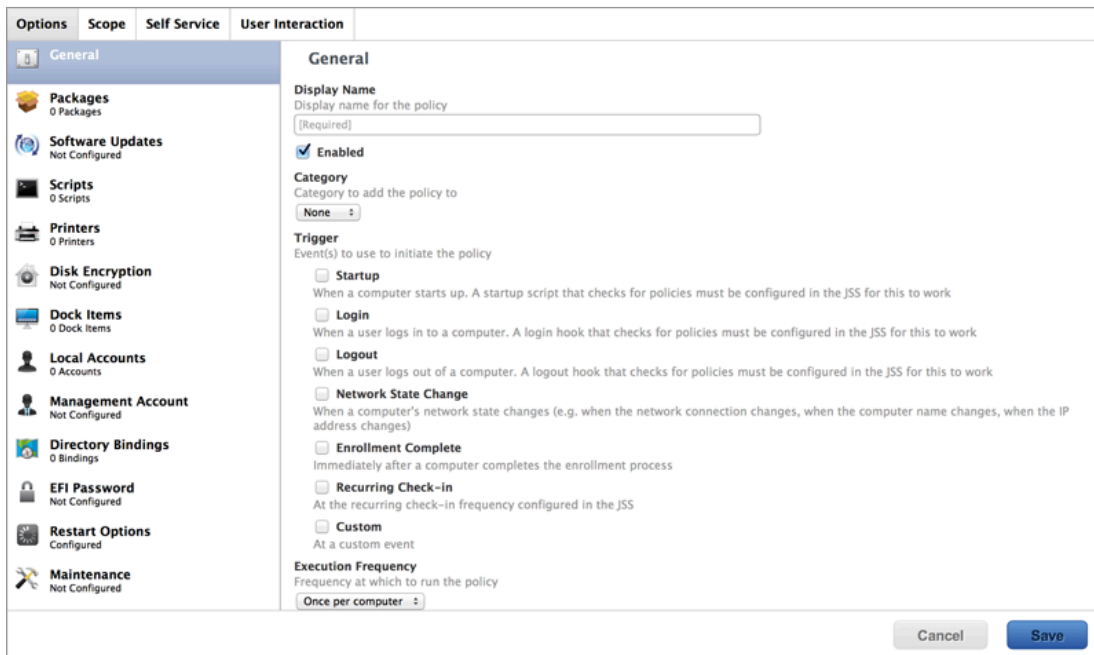
5. Click **OK**.

Step 2: Cache the InstallESD.dmg File

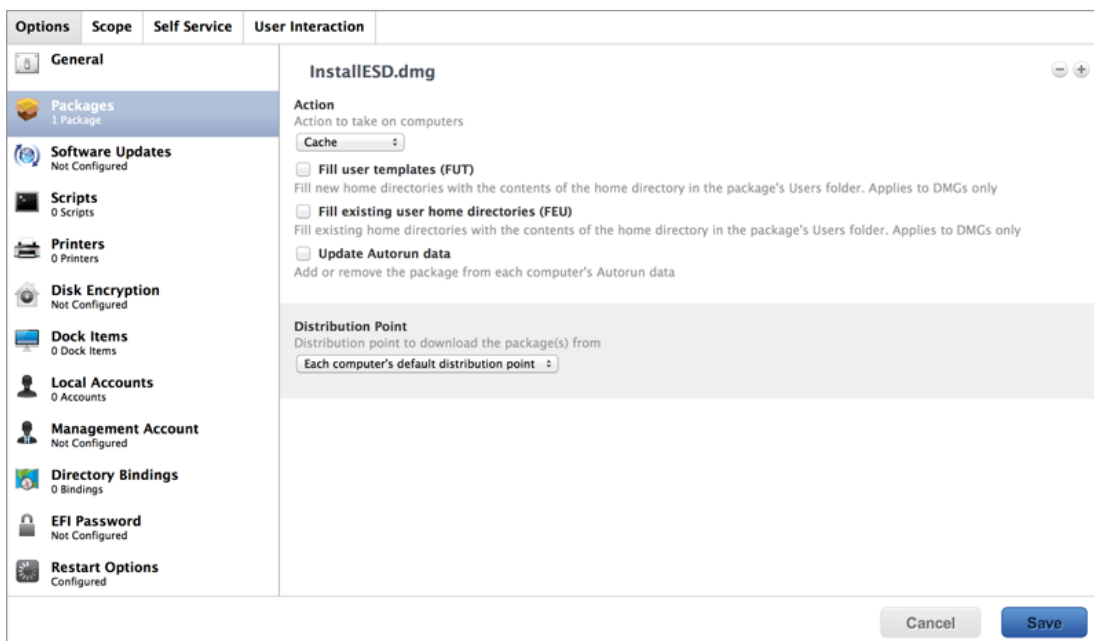
After adding the .app file to Jamf Admin, you can cache the `InstallESD.dmg` file using a policy. Caching the file ahead of time speeds up the upgrade process.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
On a smartphone, this option is in the pop-up menu.
4. Click **New**  .

- In the General payload, enter a display name for the policy. For example, "Cache InstallESD.dmg".



- Select **Recurring Check-in** as the trigger.
- Choose "Once per Computer" from the **Execution Frequency** pop-up menu.
- Select the Packages payload and click **Configure**.
- Click **Add** for the InstallESD.dmg file.
- Choose "Cache" from the **Action** pop-up menu.



- Specify a distribution point for computers to download the package from.


12. Select the Maintenance payload and click **Configure**.
13. Ensure that the **Update Inventory** checkbox is selected.
14. Click the **Scope** tab and configure the scope of the policy.


15. Click **Save**.

The `InstallESD.dmg` file is cached on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload.

Step 3: Create a Smart Computer Group


Create a smart group of computers with the `InstallESD.dmg` file cached. The smart group will be used as the scope of the Self Service policy for upgrading macOS.

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. On the Computer Group pane, enter a display name for the smart computer group. For example, "InstallESD.dmg Cached".

6. Click the **Criteria** tab.
7. Click **Add** .
8. Click **Choose** for "All Criteria".
9. Click **Choose** for "Cached Packages".


10. Choose “has” from the **Operator** pop-up menu.

And/Or	Criteria	Operator	Value
	Cached Packages	has	

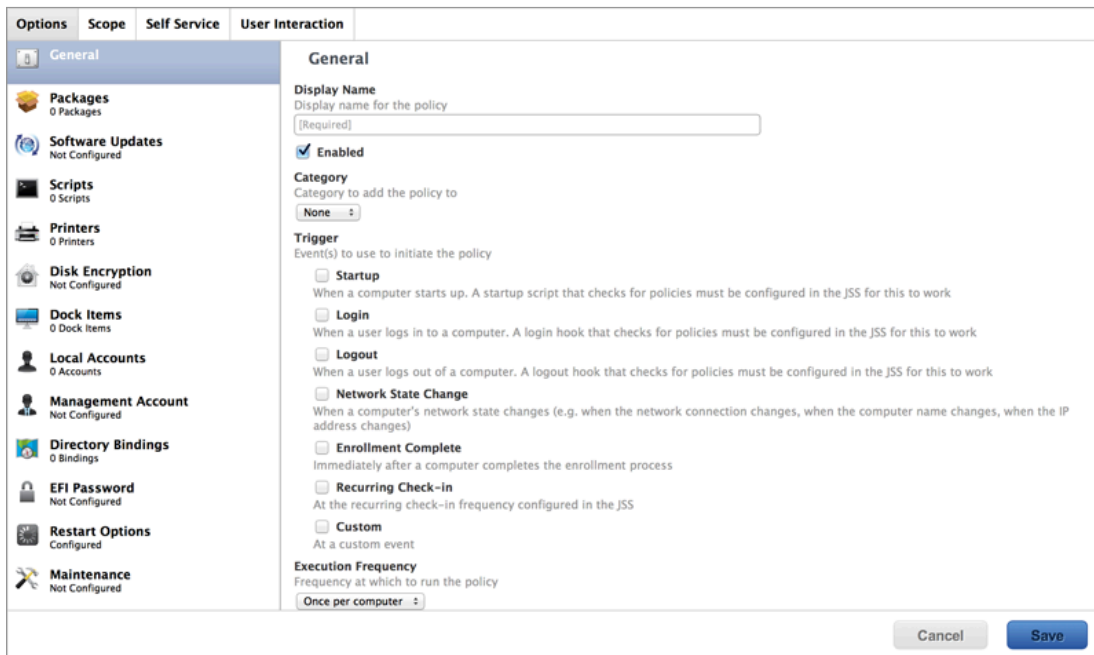
11. Click **Browse** .
12. Click **Choose** for the `InstallESD.dmg` file.
Note: The `InstallESD.dmg` file is not available as a value until it has been cached on at least one computer.
13. Click **Save**.

Step 4: Create a Self Service Policy for Upgrading macOS

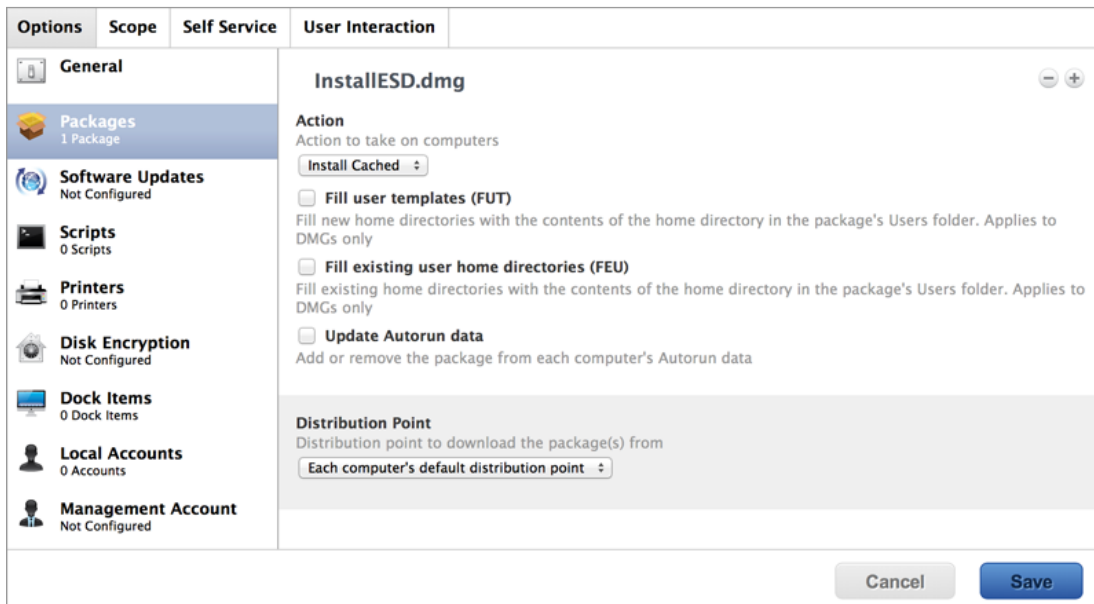
After caching the `InstallESD.dmg` file, you can create a Self Service policy that allows users to upgrade macOS.


1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .

- In the General payload, enter a display name for the policy. For example, "Upgrade macOS".



- Choose "Once per Computer" from the **Execution Frequency** pop-up menu.
- Select the Packages payload and click **Configure**.
- Click **Add** for the `InstallESD.dmg` file.
- Choose "Install Cached" from the **Action** pop-up menu.



- Click the **Scope** tab.
- Click **Add** .
- Click the **Computer Groups** tab.

13. Click **Add** for the smart computer group you just created.

Options Scope **Self Service** User Interaction

Add Deployment Targets

Computers Computer Groups Buildings Departments

Group Name

All Managed Clients Add

All Managed Servers Add

InstallESD.dmg Cached Add

Done

Cancel Save

14. Click the **Self Service** tab.
15. Select **Make the policy available in Self Service**.
16. Configure how the policy is displayed in Self Service using the settings on the pane.

Options Scope **Self Service** User Interaction

Make the policy available in Self Service

Button Name
Name for the button that users click to initiate the policy

Install

Description
Description to display for the policy in Self Service

Ensure that users view the description
Force users to view the description before the policy runs

Icon
Icon to display for the policy in Self Service. It is recommended that you use a file with the GIF or PNG format. The recommended size is 128x128 pixels

Upload Icon

Select Existing Icon

Feature the policy on the main page

Categories
Categories in which to display or feature the policy in Self Service

Display in Feature in

Cancel Save

17. Click **Save**.

The policy is made available in Self Service on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload. macOS is upgraded when users run the policy from Self Service.

Upgrading FileVault 2-enabled drives from macOS 10.7 or 10.8 prompts users to enter their password after reboot. Upgrading FileVault 2-enabled drives from macOS 10.9 or later automatically bypasses authentication after reboot.

Note: The Jamf Binary automatically enables Core Storage on the target computer before installing an macOS 10.11 upgrade using a policy. This *only* occurs for macOS 10.11 upgrades that are installed using a policy.

Deploying macOS by Imaging

Deploying macOS by imaging involves the following steps:

1. Prepare to image a partition.
2. Image computers.


Requirements

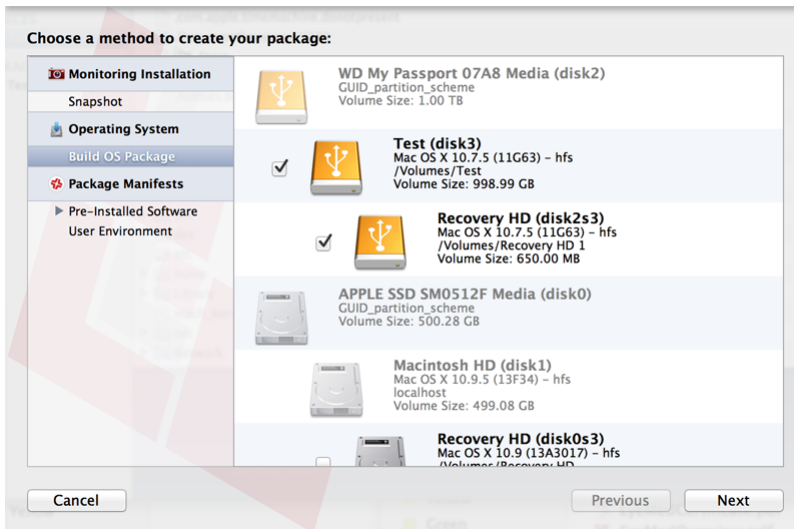
To deploy macOS by imaging, you need:

- Jamf Pro 9.7 or later
- A test computer with:
 - Composer
 - A “Recovery HD” partition
- Jamf Admin
- A distribution point
- A startup disk other than the target drive that has Jamf Imaging installed
Some common startup disks used for imaging are USB or FireWire drives, Restore partitions, and NetBoot images.

Step 1: Prepare to Image a Partition

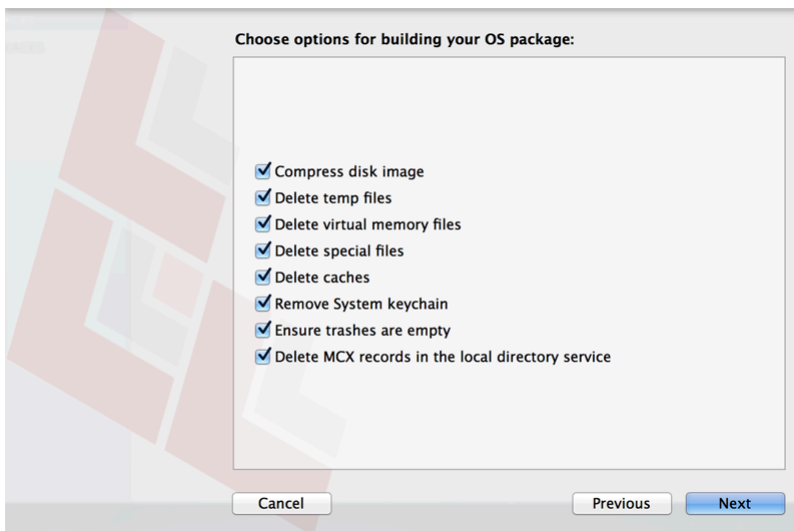
As of macOS 10.7, newly purchased Macs come with a “Recovery HD” partition that can be used for recovery tasks, such as repairing disks or reinstalling macOS. As of Jamf Pro 9.7, you have the option to build a deployable package of an operating system, a “Recovery HD” partition, or a whole disk in a single step.

1. Build an OS package:
 - a. On the test computer, install and configure the OS.
For complete instructions, see the [Creating a Minimal Base OS Image](#) Knowledge Base article.
 - b. Open Composer and authenticate locally.
 - c. In the toolbar, click **New** .
 - d. Under the Operating System heading in the sidebar, select **Build OS Package**.
For information on how Composer 9.7 or later displays partitions when building OS packages, see the [How Composer Displays Partitions when Building OS Packages](#) Knowledge Base article.
 - e. Select the drive or drives you want to package and click **Next**.



Important: It is recommended that the macOS version of the “Recovery HD” partition matches the macOS version of the OS partition.

- f. Choose options for removing unnecessary files from the package and click **Next**.

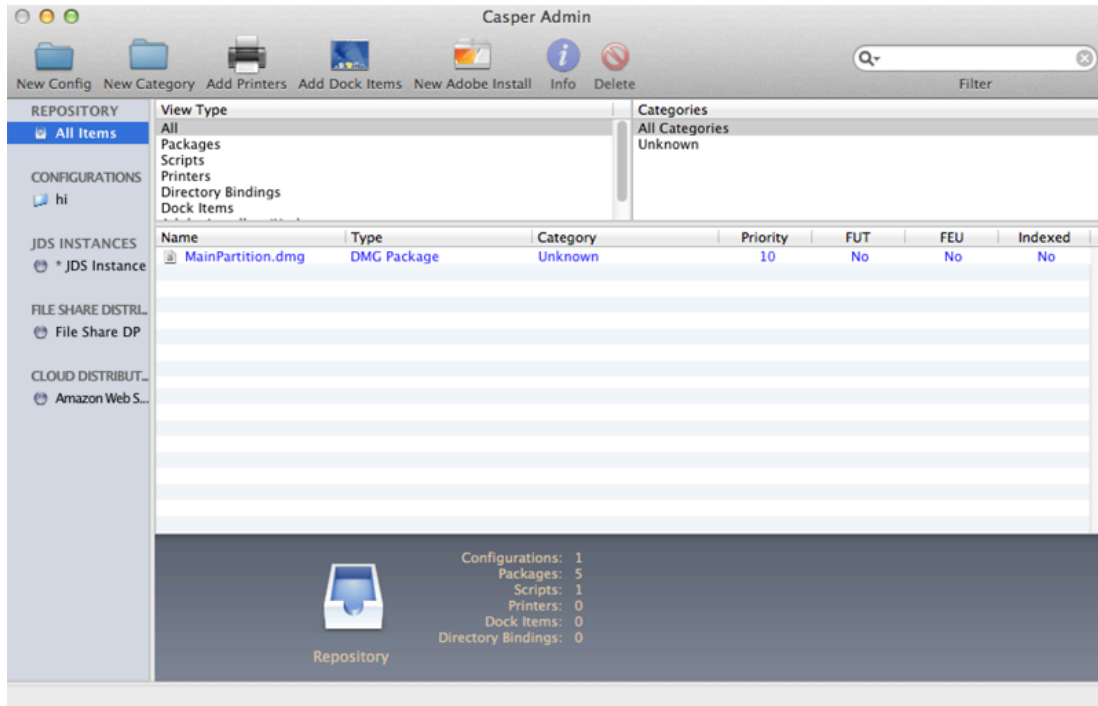


- g. Enter a package name and select a location to save the package, and then click **Build**.

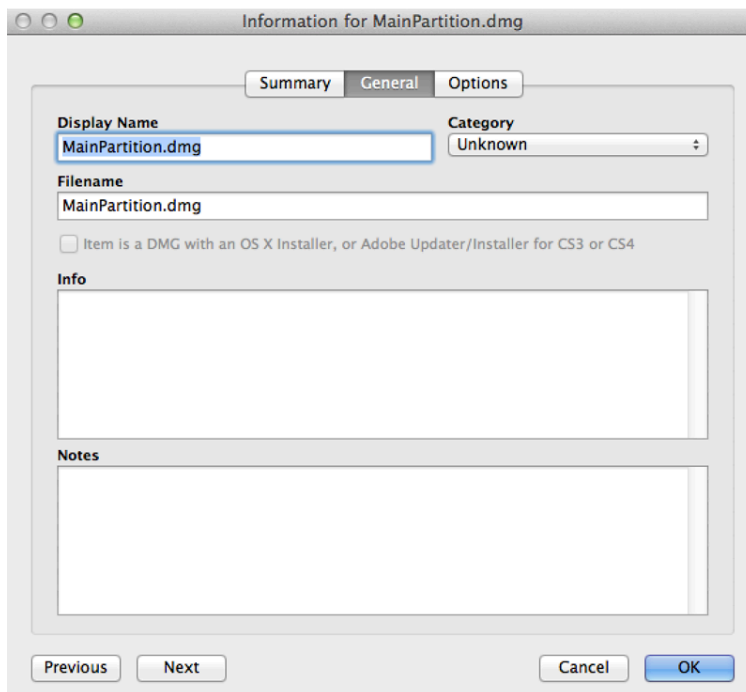
2. Add the OS package to Jamf Admin:

- a. Open Jamf Admin and authenticate to the Jamf Pro server.

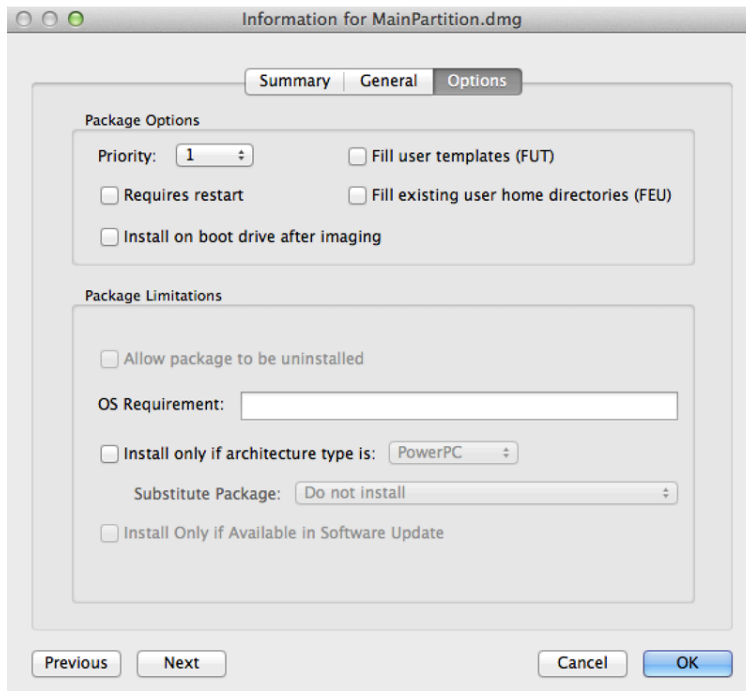
- b. Drag the package to the main repository in Jamf Admin.
The package is displayed in blue text until you add it to a category.



- c. Double-click the package in the main repository.
d. Click the **General** tab and choose a category for the package.

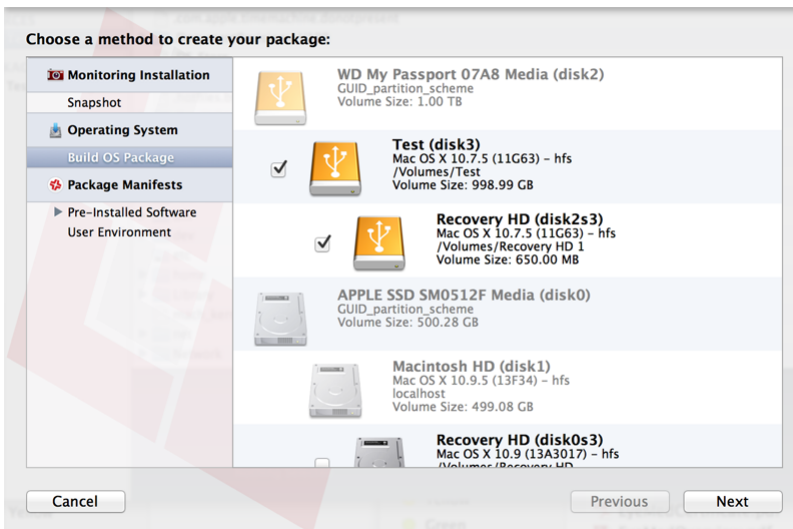


- e. Click the **Options** tab and choose a priority for the package. The recommended priority is "1".




- f. Click **OK**.

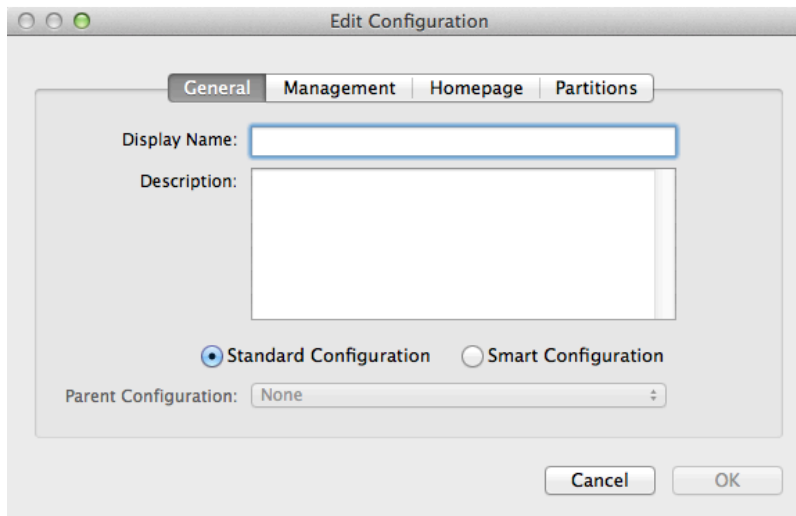
3. Create a configuration:



Note: Compiling a configuration with a multi-partition DMG will result in a DMG with a single partition.

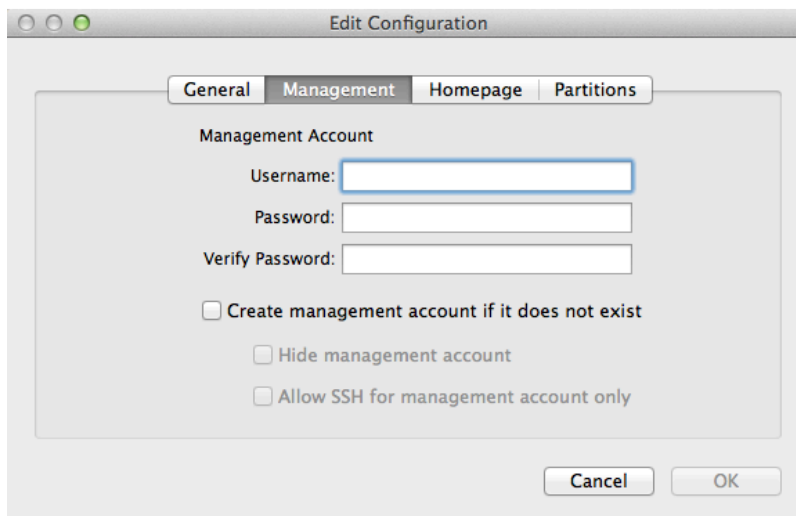
- a. Open Jamf Admin and authenticate to the Jamf Pro server.
- b. Click **New Config**  .

- c. On the General pane, enter a display name for the configuration.



The screenshot shows the 'Edit Configuration' dialog box with the 'General' tab selected. The 'Display Name' field is highlighted with a blue border. Below it is a larger 'Description' text area. At the bottom, there are two radio buttons: 'Standard Configuration' (selected) and 'Smart Configuration'. Below the radio buttons is a 'Parent Configuration' dropdown menu set to 'None'. At the bottom right are 'Cancel' and 'OK' buttons.

- d. Click the **Management** tab and enter credentials for a local administrator account that you want to use for management.



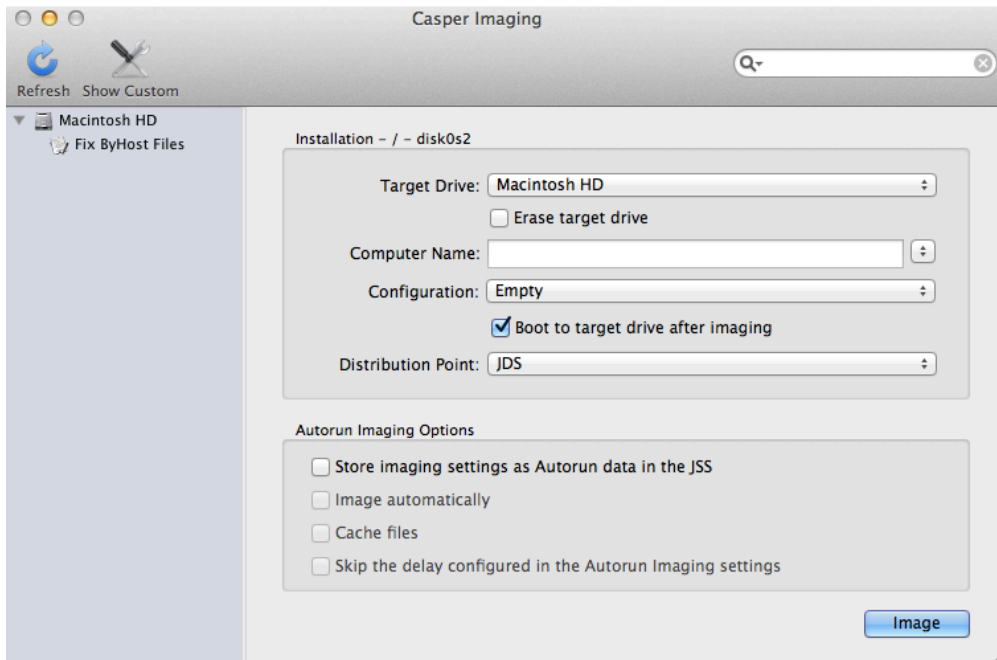
The screenshot shows the 'Edit Configuration' dialog box with the 'Management' tab selected. The 'Management Account' section contains three text input fields: 'Username', 'Password', and 'Verify Password'. Below these fields are three checkboxes: 'Create management account if it does not exist' (unchecked), 'Hide management account' (unchecked), and 'Allow SSH for management account only' (unchecked). At the bottom right are 'Cancel' and 'OK' buttons.

- e. Click **OK**.
The configuration is added to the list of configurations in the sidebar.
- f. Drag the OS package from the main repository to the configuration that you just created.

Step 2: Image Computers

1. On a target computer, boot to a startup disk other than the target drive.
2. Open Jamf Imaging and authenticate locally.
3. Authenticate to the Jamf Pro server when prompted.

4. Choose the drive to image from the **Target Drive** pop-up menu.



5. Select the **Erase target drive** checkbox.
6. Assign a name to the computer by entering a name in the **Computer Name** field.
7. From the **Configuration** pop-up menu, choose the configuration you created in "Step 1: Preparing to Image a Partition".
8. Select the **Boot to target drive after imaging** checkbox.
9. Choose a distribution point from the **Distribution Point** pop-up menu.
10. Click **Image**.
11. Repeat as needed for other target computers.

Revision History

Revision Date	Changes
11 March 2019	Updated for use with macOS 10.12 deployments. Removed the "Deploying OS X by Imaging Using the JSS 9.66 or Earlier" section.
08 April 2016	Added information on naming conventions of the <code>InstallESD.dmg</code> file.
05 February 2016	Added information on authentication action after reboot when a FileVault 2-enabled drive is upgraded.
30 September 2015	Updated for use with macOS 10.11 deployments.
07 May 2015	"Deploying macOS by Imaging Using the JSS v9.66 or Earlier" section: Updated procedure for preparing to create or modify a "Recovery HD" partition during imaging.
25 March 2015	"Deploying an macOS Upgrade" section: Added a link to a Knowledge Base article from Apple that contains system requirements for macOS 10.10. Added the "Deploying macOS by Imaging Using the JSS v9.7 or Later" section.
11 November 2013	"Deploying an macOS Upgrade" section: <ul style="list-style-type: none"> ▪ Added a link to a Knowledge Base article from Apple that contains system requirements for macOS 10.9. ▪ Removed the note about the known issue that prevents drives encrypted with FileVault from being upgraded from macOS 10.7 to 10.8. This issue was fixed in 9.21. ▪ Updated procedure for adding the .app file for macOS to Casper Admin. ▪ Added a step for selecting the Update Inventory checkbox when creating a policy to cache the <code>InstallESD.dmg</code> file. "Deploying macOS by Imaging" section: Updated procedure for preparing to create or modify a "Recovery HD" partition during imaging.